PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené
ako otvorená cloudová služba s prvkami strojového učenia

V21 – Dostupné online osvetové podklady a výstupy

KPB7 – osvetové aktivity
typ – edukačné materiály
mesiac odovzdania – M22

Obsah

Úvod **3**
1 Spôsoby oslovenia a komunikačné nástroje **3**
1.1 Webová stránka *3*
1.1.1 Realizované aktivity 3
1.2 Sociálne siete *15*
1.2.1 Realizované aktivity 15
1.3 Popularizačné texty *36*
1.3.1 Realizované aktivity 36
1.4 Audiovizuálny obsah *45*
1.4.1 Realizované aktivity 46
Zoznam zdrojov **54**
Prílohy **57**
Prílohe 1 – Článok: Stretnutie partnerov 15.7.2025 ..... *57*
Príloha 2 – Článok: Základy projektu INNOSOC: Rozhovor s Ing. Michalom Papučíkom *57*
Príloha 3 – Článok: Rozhovor s prof. Ing. Pavlom Segečom, PhD.: Kybernetická bezpečnosť už nie je len témou pre veľké firmy *58*
Príloha 4 – Článok: Študentská udalosť FRIčkovica – 8.októbra *59*
Príloha 5 – Oznam o konaní sympózia INNOSOC *59*
Príloha 6 – Článok o vyhlásení víťaza súťaže o iPad *59*
Príloha 7 – Článok: Prezentácia projektu INNOSOC na študentských raňajkách *59*
Príloha 8 – Článok o prezentácii projektu na fakulte Aplikovanej informatiky na Univerzite Tomáše Báti v Zlíne . *59*
Príloha 9 – Článok o prezentácii projektu INNOSOC na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici *60*
Príloha 10 – Článok: Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami *60*
Príloha 11 – Článok: Security Operations Center: čo to je a ako chráni vašu firmu? *62*
Príloha 12 – Článok: Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany *63*
Príloha 13 – Článok: Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska *65*
Príloha 14 – Článok: Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady *67*
Príloha 15 – Rozhovor s Ing. Michalom Papučíkom *69*
Príloha 16 – Rozhovor s prof. Ing. Pavlom Segečom, PhD. *70*
Príloha 17 - Článok o rozhovore s odborníkmi Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakonm, PhD .. *72*
Príloha 18 - Článok o rozhovore o projekte INNOSOC: Kybernetická bezpečnosť a rozširovanie obzorov s Dominikou Toman *73*
Príloha 19 - Článok o rozhovore o projekte INNOSOC: O vedeckom výskume a kybernetickej bezpečnosti s Martinom Mičiakom *73*
Príloha 20 – Článok o prof. Ing. Milanom Kubinom, PhD. o projekte INNOSOC *74*
Príloha 21 – Popularizačný článok na tému Prepojenie AI a kybernetickej bezpečnosti v praxi *75*
Príloha 22 – Popularizačný článok na tému Kybernetické útoky: Ako sa menia a prečo predstavujú čoraz väčšie riziko *77*
Príloha 23 – Popularizačný článok na tému Automatizácia a hlboké strojové učenie v kybernetickej bezpečnosti *79*
Príloha 24 – Rozhovor s Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD. *81*
Príloha 25 – Rozhovor s Ing. Martinom Mičiakom, PhD. *83*
Príloha 26 – Rozhovor s Ing. Dominikou Toman, PhD. *84*
Príloha 27 – Rozhovor s prof. Ing. Milan Kubina, PhD. *84*

Úvod

Dokument obsahuje prehľad a popis dostupných online osvetových aktivít spojených s projektom INNOSOC. Aktivity a výstupy ktoré zo svojej podstaty neboli dostupné online sú popísané vo výstupe V22 - Zrealizované osvetové aktivity.

1 Spôsoby oslovenia a komunikačné nástroje

Efektívna osvetová kampaň projektu INNOSOC si vyžaduje cielenú a diferencovanú komunikáciu naprieč viacerými cieľovými skupinami. Na to, aby sa obsah a posolstvo projektu dostali k študentom, odbornej verejnosti, laickej verejnosti aj potenciálnym zákazníkom, musia byť využité viaceré formáty a kanály komunikácie.

Základným princípom je kombinácia digitálnej prítomnosti, odborných a populárno-náučných publikácií, ako aj fyzického materiálu pre osobné stretnutia a podujatia. V tejto kapitole predstavujeme jednotlivé komunikačné nástroje, ktoré budú využívané v rámci projektu.

1.1 Webová stránka

Webová stránka projektu slúži ako základný komunikačný a informačný kanál, prostredníctvom ktorého sa verejnosti sprostredkúvajú hlavné informácie o projekte. Jej hlavným účelom je predstaviť ciele, odborné zameranie a inovatívny charakter riešenia, ktoré projekt prináša v oblasti kybernetickej bezpečnosti a cloudových technológií.

Slúži na to, aby záujemcom poskytla prehľad o výskumnej orientácii, prínosoch pre prax a súvislostiach s európskymi digitálnymi iniciatívami.

Stránka zároveň poskytuje základné informácie o zapojených partneroch, ich rolách a o kontexte, v ktorom projekt vznikol. Plní úlohu úvodného bodu, kde sa návštevníci môžu oboznámiť s projektom a následne sledovať jeho ďalší vývoj – najmä prostredníctvom pravidelnej aktualizácie obsahu v podobe noviniek alebo výstupov.

Stránka rástla a dopĺňala sa o ďalšie sekcie: odborné a popularizačné články, dokumenty na stiahnutie, vizualizácie riešenia, výskumné výstupy, ako aj výzvy na zapojenie verejnosti či študentov. Je zároveň prepojená na sociálne siete, kde sa zdieľajú aktuality a osvetové aktivity zamerané na rôzne cieľové skupiny. Webová stránka teda slúži ako otvorená a postupne rozvíjaná platforma, ktorá podporuje transparentnosť, informovanosť a budovanie záujmu o tému kybernetickej bezpečnosti.

1.1.1 Realizované aktivity

1.1.1.1 Tvorba webovej stránky

Pre účely komunikácie so širokou verejnosťou bola vytvorená webová stránka INNOSOC. Stránka sa skladá z 5 základných sekcií, medzi ktorými sa môže používateľ pohybovať, a to sú: **Domov, O projekte, Výstupy, Novinky, Kontakt**.

Po príchode na webovú stránku je používateľovi viditeľný stručný opis projektu. Stránka obsahuje logá vykonávateľov, trvanie projektu aj partnerov, ktorí na projekte pracujú.

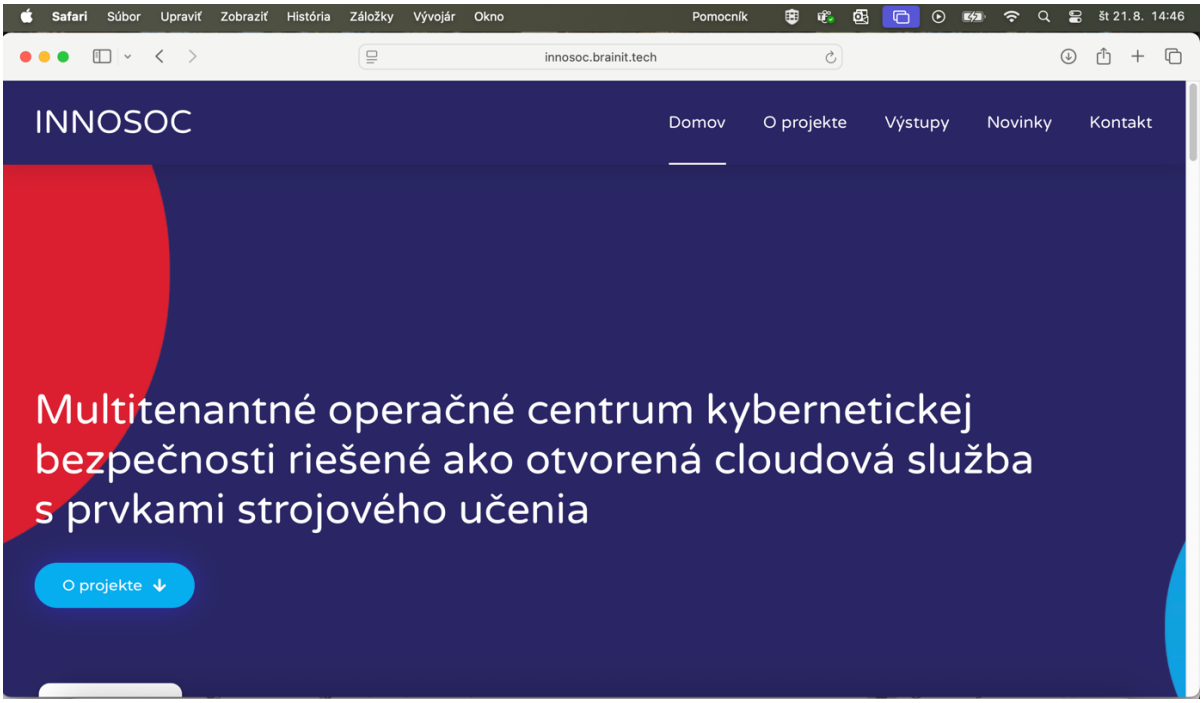
Sekcia „Domov“ komunikuje hlavný cieľ projektu, čiastkové ciele, výzvy, ktoré k projektu viedli ako aj jeho prínos a segmenty, ktoré budú z výstupov projektu benefitovať.

Používateľ sa o projekte dozvie viac po rozkliknutí na sekciu „O projekte“, kde je podrobne rozpísaný cieľ projektu ako aj jeho identifikačné údaje, ako je kód výzvy, názov investície, názov komponentu, kód projektu, miesto realizácie, termín realizácie.

Na webovej stránke sú dostupné aj všetky výstupy vo forme projektovej dokumentácie, reportov z experimentov a testovania, návody aj záverečná správa. Všetky tieto dokumenty sa budú na webovú stránku postupne nahrávať a budú dostupné na prehliadanie.

Ďalšou sekciou sú „Novinky“, kde boli zverejňované blogové články, popularizačné články ako aj všetky novinky, ktoré sa týkajú realizovaných aktivít, stretnutí či publikovaných indexových článkov a publikácií.

Poslednou dostupnou sekciou je „Kontakt“, kde má používateľ prístupný formulár v prípade otázok.

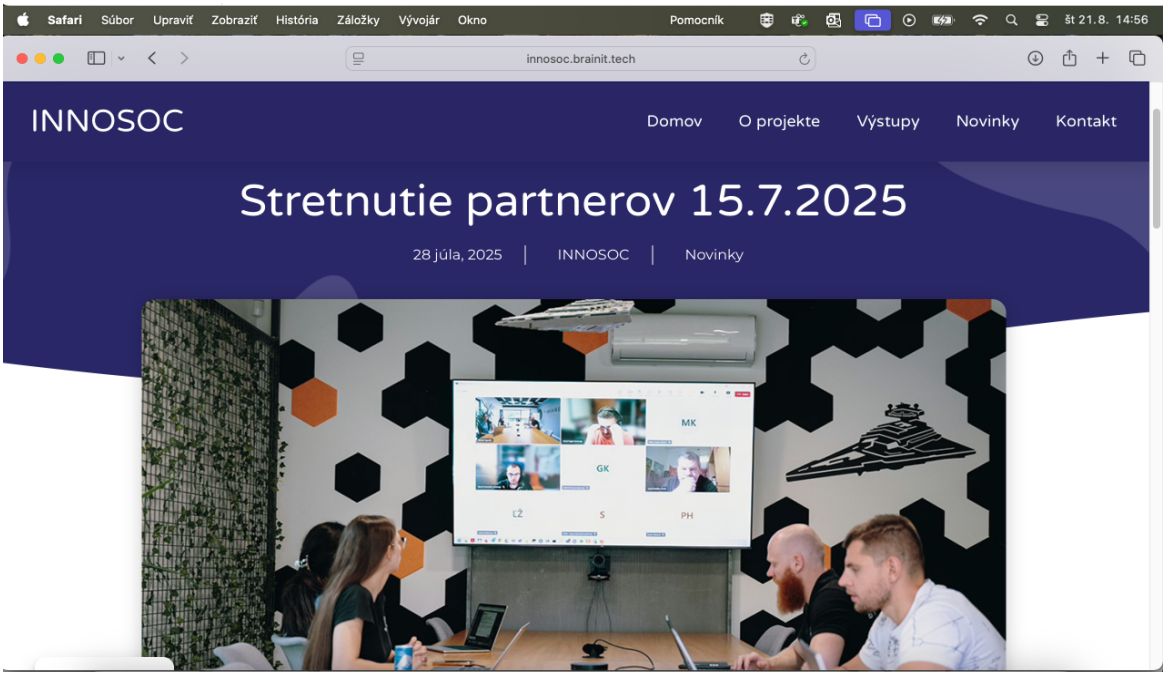


Obrázok 1: Náhľad úvodnej stránky INNOSOC, Zdroj: (BRAIN:IT, 2025)

1.1.1.2 Článok o stretnutí partnerov

Cieľom blogového príspevku uverejneného dňa 28. júla 2025 bolo komunikovať priebeh stretnutí partnerov projektu, spoločnosti BRAIN:IT a Fakulty riadenia a informatiky, Žilinskej univerzity v Žiliny širokej verejnosti. Článok o stretnutí z 15.7.2025 komunikuje aktuálny priebeh prác na projekte, ďalšie smerovanie aj organizačné aktivity na nasledujúce obdobie, ktoré sa riešili online stretnutím.

Celé znenie článku sa nachádza v prílohe 1 – Článok: Stretnutie partnerov 15.7.2025

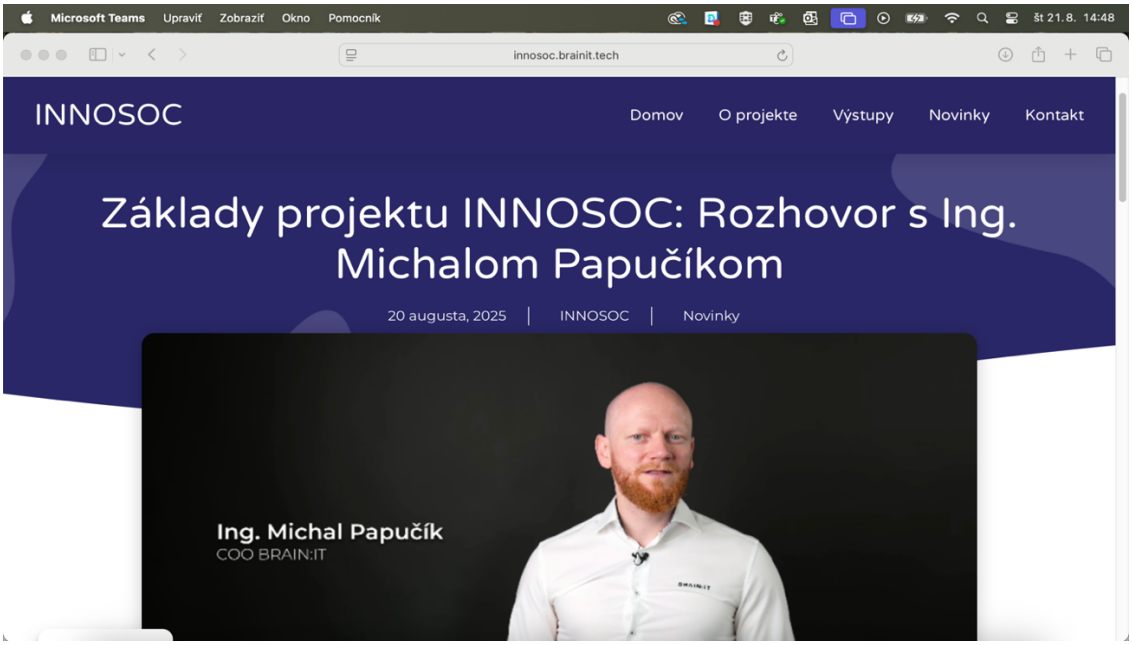


Obrázok 2: Článok na webovej stránke INNOSOC: Stretnutie partnerov 15.7.2025, Zdroj: (BRAIN:IT, 2025)

1.1.1.3 Článok o rozhovore s Ing. Michalom Papučíkom

Do sekcie „Novinky“ bol 20. augusta pridaný krátky článok, ktorý komunikuje informačné video, rozhovor, ktorý bol natočený s COO spoločnosti BRAIN:IT, Ing. Michalom Papučíkom. Do článku je video vložené prostredníctvom zdieľania z kanálu @INNOSOC na platforme YouTube. Blogový článok pomáha distribuovať informáciu o rozhovore širšej verejnosti a zároveň tak rozšíriť povedomie o základných informáciách o projekte INNOSOC.

Celé znenie článku sa nachádza v prílohe 2 – Článok: Základy projektu INNOSOC: Rozhovor s Ing. Michalom Papučíkom.



Obrázok 3: Článok na webovej stránke INNOSOC: Základy projektu INNOSOC, Zdroj: (BRAIN:IT, 2025)

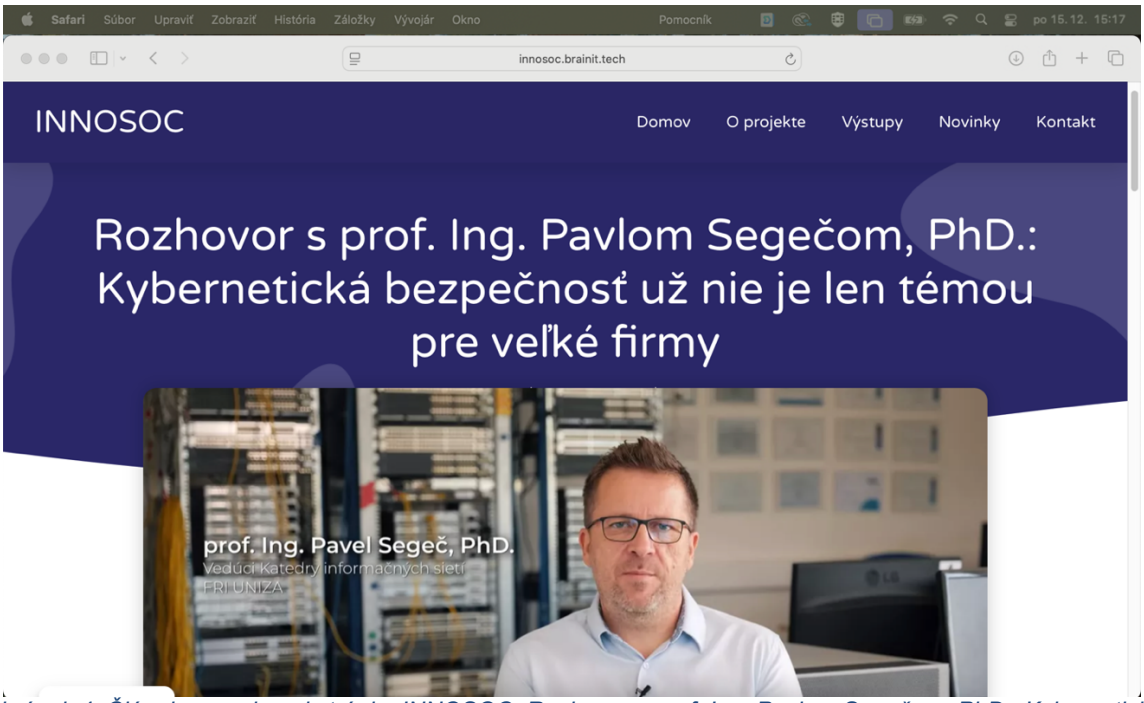
1.1.1.4 Článok o rozhovore s prof. Ing. Pavlom Segečom, PhD.

V rámci projektu bol dňa realizovaný a publikovaný odborný rozhovor s prof. Ing. Pavlom Segečom, PhD., vedúcim Katedry informačných sietí na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline (UNIZA), ktorý pôsobí ako kľúčový vedecko-výskumný pracovník projektu. Cieľom rozhovoru bolo priblížiť význam kybernetickej bezpečnosti v súčasnom digitálnom prostredí, poukázať na rastúce kybernetické hrozby a vysvetliť úlohu projektu INNOSOC pri budovaní systematickej a centralizovanej ochrany organizácií a vzdelávacích inštitúcií. Obsah rozhovoru sa zameriava najmä na:

- význam kybernetickej bezpečnosti pre organizácie všetkých veľkostí v kontexte rastúcej digitalizácie,
- úlohu Fakulty riadenia a informatiky UNIZA ako hlavného partnera projektu a poskytovateľa vedecko-výskumných a vývojových kapacít,
- identifikáciu najčastejších kybernetických hrozieb, ako sú phishing, ransomvér a pokročilé pretrvávajúce hrozby (APT),
- vysvetlenie konceptu Security Operations Center (SOC) ako centrálneho prvku ochrany, postaveného na pilieroch ľudí, procesov a technológií,
- dopady novej smernice NIS2 na požiadavky v oblasti riadenia a reportovania kybernetických incidentov,
- praktické fungovanie SOC systémov založených na zbere, korelácii a analýze veľkého objemu bezpečnostných dát v reálnom čase.

Rozhovor predstavuje odborný, prezentačný a osvetový výstup projektu, ktorý prepája vedecko-výskumný pohľad s praktickými dopadmi na bezpečnosť organizácií. Zároveň slúži ako nástroj na zvyšovanie povedomia o význame kybernetickej bezpečnosti a o prínosoch projektu INNOSOC pre akademickú aj aplikačnú prax.

Celé znenie článku sa nachádza v prílohe 3 – Článok: Rozhovor s prof. Ing. Pavlom Segečom, PhD.: Kybernetická bezpečnosť už nie je len témou pre veľké firmy.



Obrázok 4: Článok na webovej stránke INNOSOC: Rozhovor s prof. Ing. Pavlom Segečom, PhD.: Kybernetická bezpečnosť už nie je len témou pre veľké firmy, Zdroj: (BRAIN:IT, 2025)

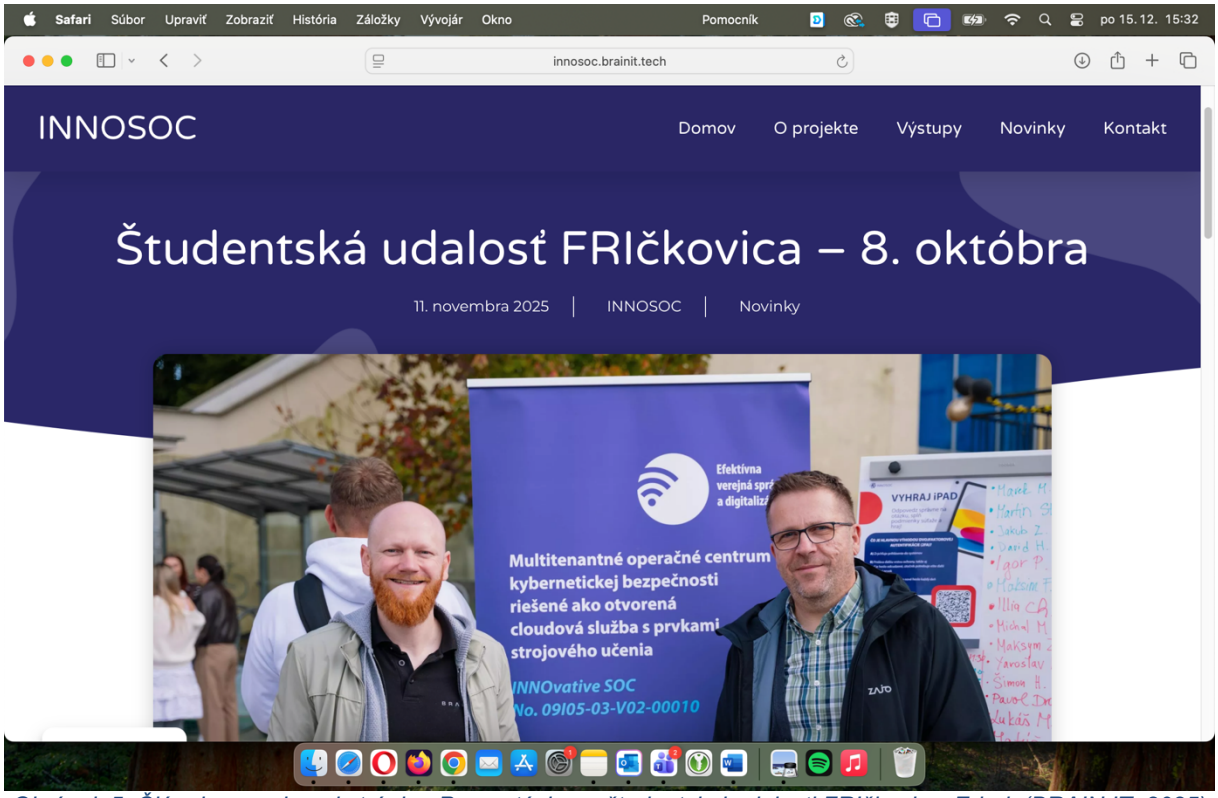
1.1.1.5 Článok o prezentovaní projektu INNOSOC na študentskej udalosti FRIčkovica

Dňa 11. novembra 2025 bol v sekcii „Novinky“ zverejnený článok o prezentácii projektu INNOSOC na študentskej udalosti FRIčkovica, ktorá sa konala dňa 8. októbra 2025 na Fakulte riadenia a informatiky na Žilinskej univerzite v Žiline. Cieľom účasti projektu na podujatí bolo priblížiť študentom projekt INNOSOC, jeho hlavné zámery, ciele a riešené problémy v oblasti kybernetickej bezpečnosti, ako aj zvýšiť povedomie o význame výskumu a inovácií v tejto oblasti.

V rámci aktivity bol pre študentov pripravený informačný a prezentačný stánok, prostredníctvom ktorého boli komunikované hlavné výstupy projektu, jeho prínosy pre akademickú aj aplikačnú prax a možnosti zapojenia sa do problematiky kybernetickej bezpečnosti. Prezentácia zároveň slúžila ako nástroj popularizácie témy kybernetickej bezpečnosti medzi mladými odborníkmi a študentmi technických odborov.

Aktivita predstavuje popularizačný a diseminačný výstup projektu, zameraný na podporu vzdelávania, budovanie povedomia o kybernetickej bezpečnosti a posilnenie prepojenia medzi výskumným projektom, akademickým prostredím a študentskou komunitou.

Celé znenie článku sa nachádza v prílohe 4 – Článok: Študentská udalosť FRIčkovica – 8.októbra.



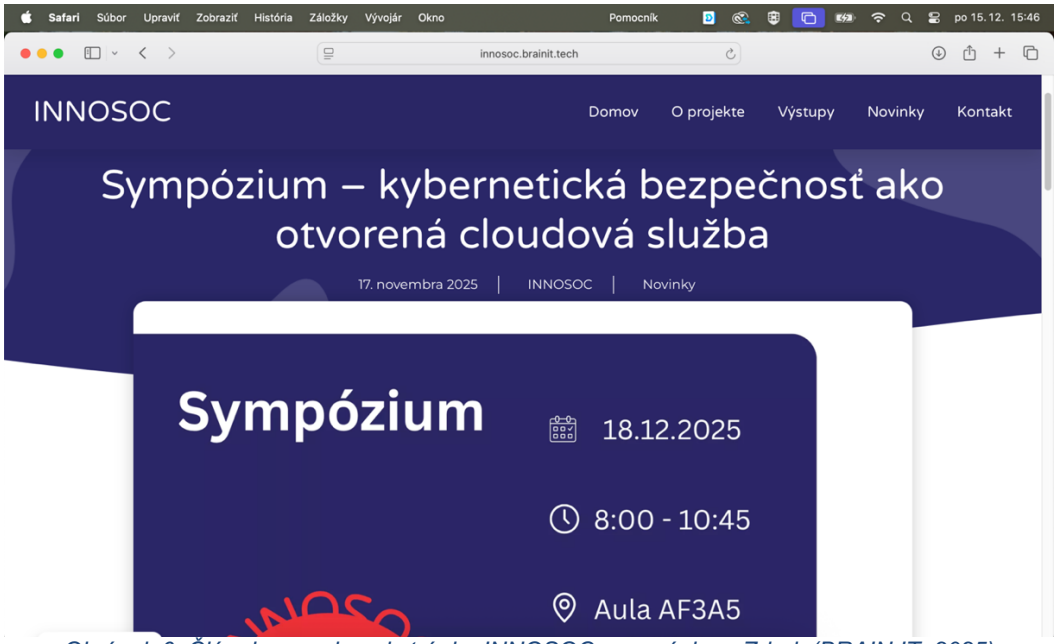
Obrázok 5: Článok na webovej stránke: Prezentácia na študentskej udalosti FRIčkovica, Zdroj: (BRAIN:IT, 2025)

1.1.1.6 Informačný oznam o konaní sympózia projektu INNOSOC

Dňa 17. novembra bol v sekcii „Novinky“ zverejnený oznam o konaní odborného sympózia na tému Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia, ktoré sa uskutoční dňa 19. decembra 2025 v priestoroch Žilinskej univerzity v Žiline. Cieľom sympózia bolo prezentovať aktuálny stav riešenia projektu INNOSOC, jeho priebežné

výsledky a výskumné zistenia v oblasti kybernetickej bezpečnosti a cloudových bezpečnostných služieb. Podujatie vytvára priestor na odbornú diskusiu medzi akademickou obcou, výskumníkmi, študentmi a ďalšími odborníkmi z praxe.

Celé znenie oznamu na webovej stránke sa nachádza v prílohe 5 – Oznam o konaní sympózia INNOSOC.

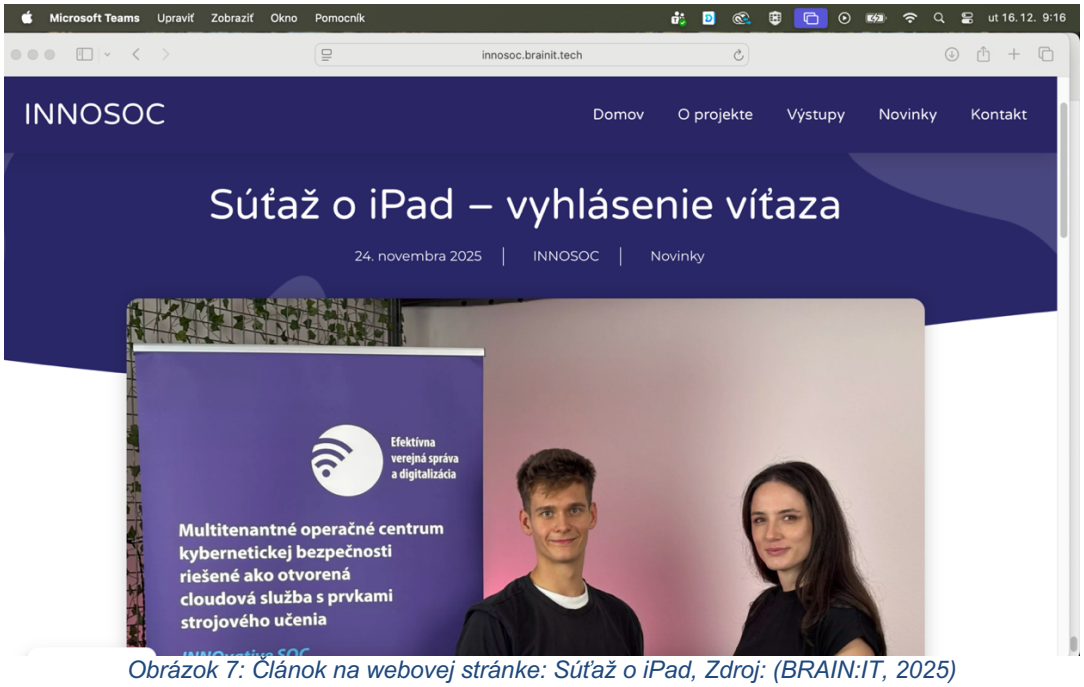


Obrázok 6: Článok na webovej stránke INNOSOC: sympózium, Zdroj: (BRAIN:IT, 2025)

1.1.1.7 Článok o vyhlásení víťaza súťaže o iPad

Dňa 24. novembra bol uverejnený článok, ktorý oznamuje vyhlásenie víťaza súťaže o iPad, ktorá bola organizovaná prostredníctvom instagramového profilu @innosoc_.

Celé znenie článku sa nachádza v prílohe 6 – Článok o vyhlásení víťaza súťaže o iPad.



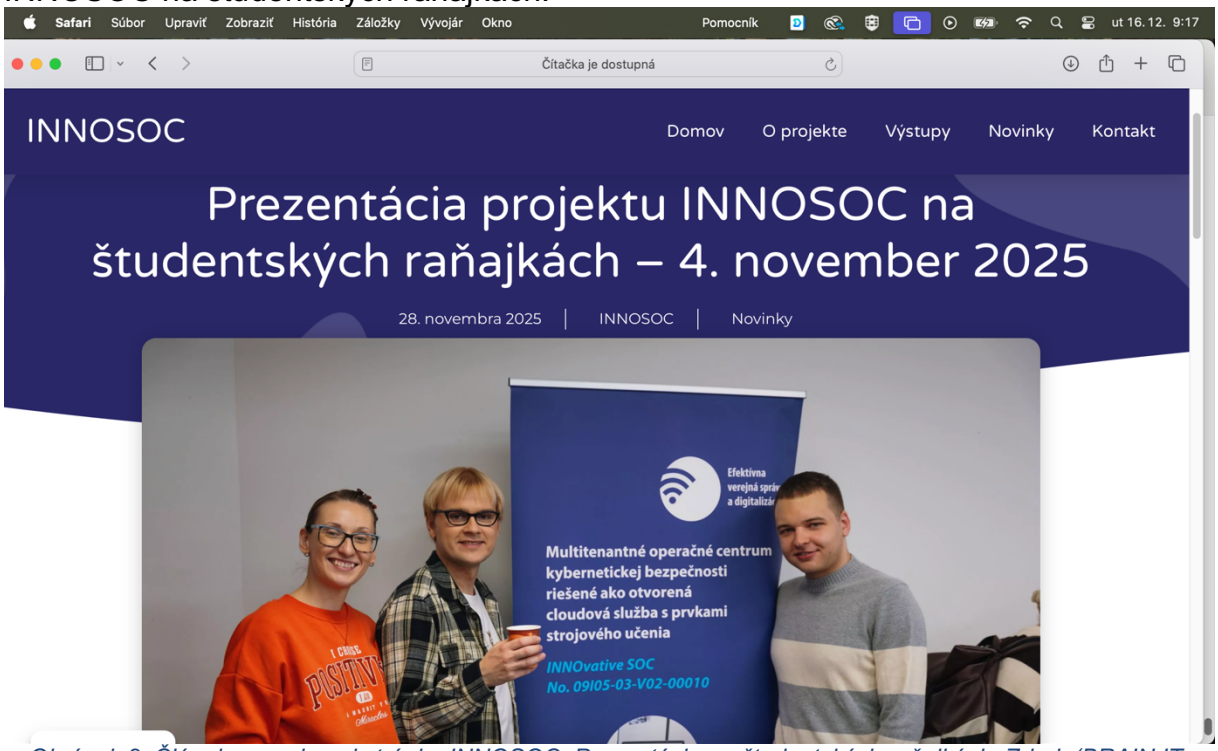
Obrázok 7: Článok na webovej stránke: Súťaž o iPad, Zdroj: (BRAIN:IT, 2025)

1.1.1.8 Článok o prezentácii projektu INNOSOC na študentských raňajkách

Dňa 28. novembra 2025 bol zverejnený článok, ktorý komunikuje prezentáciu projektu INNOSOC v rámci konania študentských raňajok na Fakulte riadenia a informatiky na Žilinskej univerzite v Žiline dňa 4. novembra. Cieľom aktivity bolo neformálnou formou predstaviť projekt INNOSOC študentom manažérskych a informatických odborov, oboznámiť ich s aktuálnym stavom riešenia projektu, jeho doterajšími výstupmi a plánovanými ďalšími krokmi. V rámci prezentácie boli zároveň komunikované kľúčové témy projektu, najmä význam kybernetickej bezpečnosti v súčasnom digitálnom prostredí, úloha Security Operations Center (SOC) a prínosy využívania cloudových technológií pri ochrane informačných systémov.

Aktivita predstavuje prezentačný, popularizačný a diseminačný výstup projektu, zameraný na zvyšovanie povedomia o kybernetickej bezpečnosti, podporu záujmu študentov o túto oblasť a posilnenie prepojenia medzi akademickým prostredím, výskumným projektom a aplikačnou praxou.

Celé znenie článku sa nachádza v prílohe 7 – Článok: Prezentácia projektu INNOSOC na študentských raňajkách.



Obrázok 8: Článok na webovej stránke INNOSOC: Prezentácia na študentských raňajkách, Zdroj: (BRAIN:IT, 2025)

1.1.1.9 Článok o prezentácii projektu na fakulte Aplikovanej informatiky na Univerzite Tomáše Báti v Zlíne

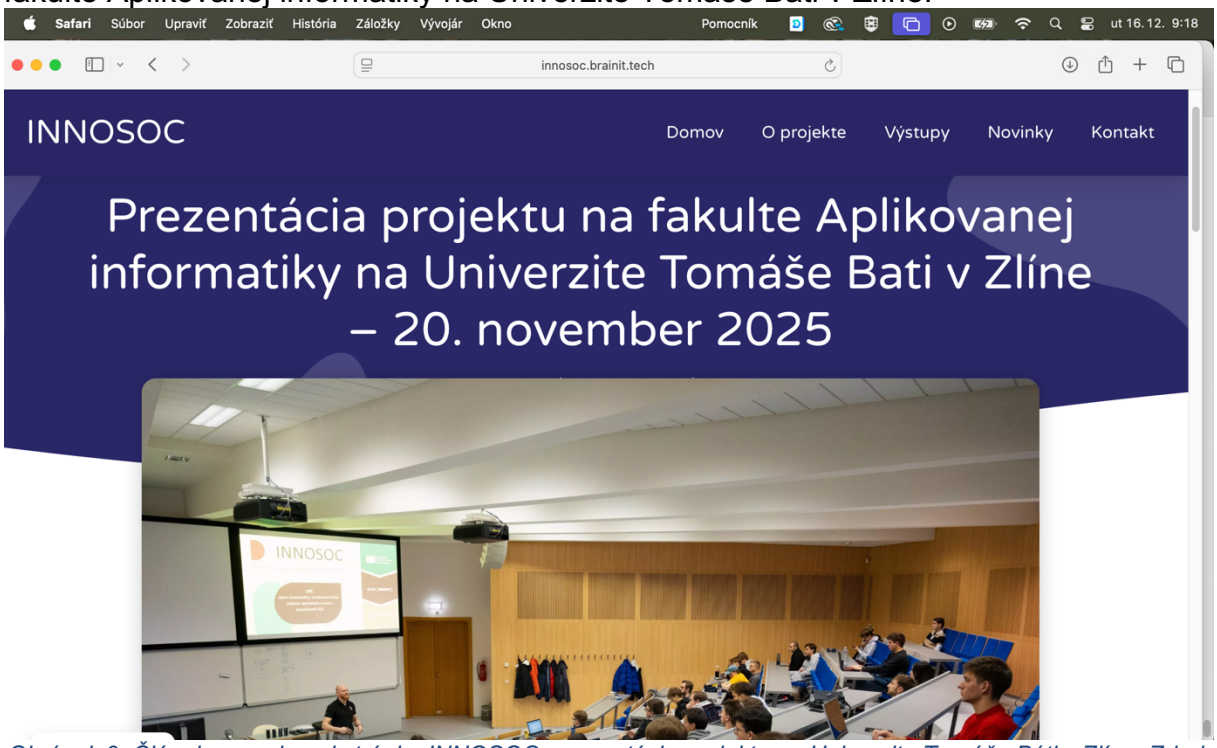
Dňa 9. decembra 2025 bol zverejnený článok, ktorý komunikuje prezentáciu projektu INNOSOC na fakulte Aplikovanej informatiky na Univerzite Tomáše Báti v Zlíne dňa 20. novembra 2025. Projekt INNOSOC bol študentom predstavený Ing. Michalom Papučíkom, ktorý priblížil hlavné ciele projektu, jeho zameranie a spôsob, akým reaguje na výzvy súvisiace s prechodom na digitálnu ekonomiku a rastúce požiadavky na kybernetickú bezpečnosť. Prezentácia sa zameriavala najmä na:

- prepojenie projektu INNOSOC s aktuálnymi potrebami komerčnej a priemyselnej sféry,

- rastúci dopyt po moderných IT službách a kvalifikovaných IT špecialistoch,
- význam zvyšovania úrovne kybernetickej bezpečnosti v organizáciách,
- základné princípy, technológie a prístupy využívané v projekte INNOSOC.

Aktivita predstavuje prezentačný, popularizačný a diseminačný výstup projektu, zameraný na šírenie výsledkov projektu, posilnenie spolupráce medzi akademickým prostredím a aplikačnou praxou a motiváciu študentov k odbornému rastu v oblasti kybernetickej bezpečnosti a informačných technológií.

Celé znenie článku sa nachádza v prílohe 8 – Článok o prezentácii projektu na fakulte Aplikovanej informatiky na Univerzite Tomáše Báti v Zlíne.



Obrázok 9: Článok na webovej stránke INNOSOC: prezentácia projektu na Univerzite Tomáše Báti v Zlíne, Zdroj: (BRAIN:IT, 2025)

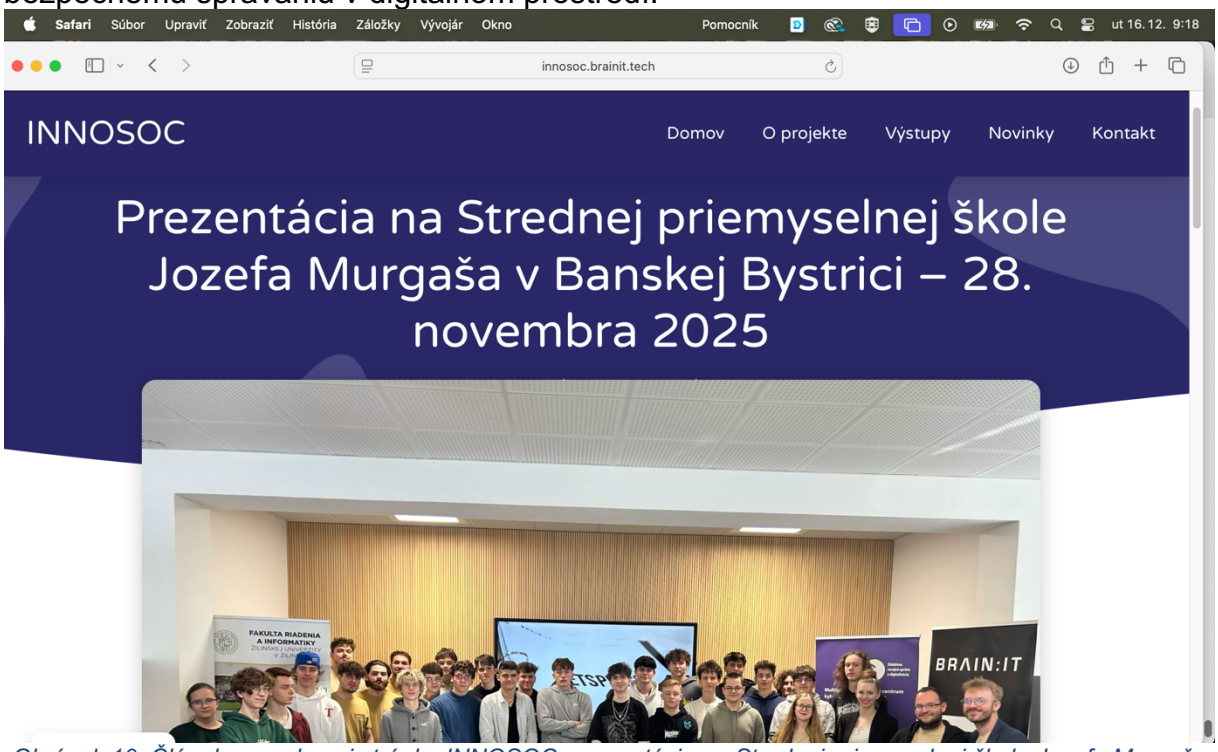
1.1.1.10 Článok o prezentácii na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici

Dňa 12. decembra bol v sekcii „Novinky“ zverejnený článok, ktorý komunikuje prezentáciu projektu INNOSOC na Strednej priemyselnej škole Joefa Murgaša v Banskej Bystrici dňa 29. Novembra 2025. Cieľom aktivity bolo priblížiť projekt INNOSOC žiakom strednej školy, vysvetliť základné princípy kybernetickej bezpečnosti a zvýšiť povedomie o digitálnych hrozbách, s ktorými sa môžu stretávať v každodennom živote. V rámci prezentácie sa žiaci oboznámili najmä s:

- hlavným zameraním a cieľmi projektu INNOSOC,
- oblasťami, ktorým sa projekt venuje,
- najčastejšími typmi kybernetických útokov v súčasnosti,
- zapojenými vzdelávacími a akademickými inštitúciami,
- významom kybernetickej bezpečnosti pre jednotlivcov aj spoločnosť.

Prezentácia bola realizovaná interaktívnou formou s dôrazom na aktívne zapojenie žiakov do diskusie, čím sa podporil ich záujem o problematiku kybernetickej bezpečnosti a rozvoj digitálnej gramotnosti.

Aktivita predstavuje popularizačný, edukačný a diseminačný výstup projektu, zameraný na osvetu v oblasti kybernetickej bezpečnosti a motiváciu mladých ľudí k bezpečnému správaniu v digitálnom prostredí.



Obrázok 10: Článok na webovej stránke INNOSOC: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici, Zdroj: (BRAIN:IT, 2025)

1.1.1.11 Článok o rozhovore s odborníkmi Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD.

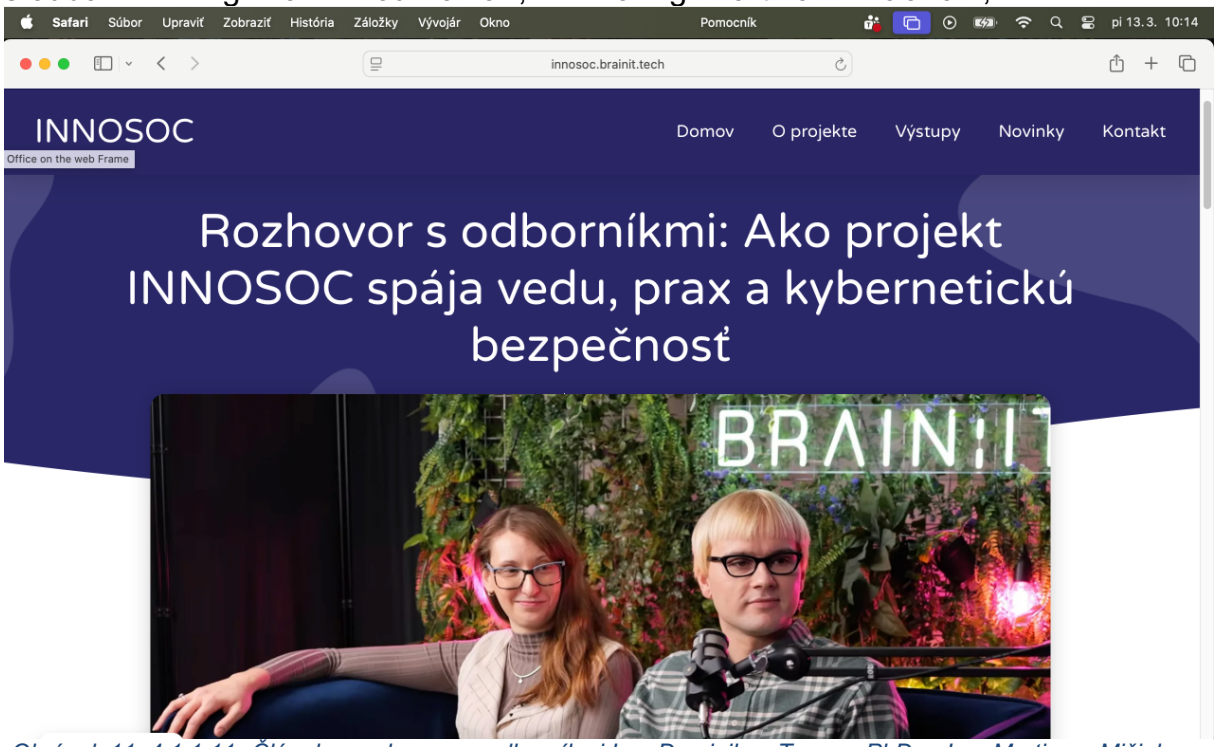
Dňa 27. januára 2026 bol na webovej stránke INNOSOC zverejnený článok s názvom „Rozhovor s odborníkmi: Ako projekt INNOSOC spája vedu, prax a kybernetickú bezpečnosť“, ktorý prezentuje odborný pohľad na význam a ciele projektu. Článok je spracovaný formou rozhovoru s odborníkmi zapojenými do projektu a približuje jeho prínosy pre výskum aj aplikačnú prax.

Hlavnou myšlienkou rozhovoru je predstavenie projektu INNOSOC ako iniciatívy, ktorá prepája akademické prostredie a priemyselnú prax s cieľom posilniť kybernetickú bezpečnosť organizácií prostredníctvom moderných technológií a výskumu. Diskusia sa zameriava najmä na význam budovania Security Operations Center (SOC), ktoré umožňuje centralizované monitorovanie, analýzu a riešenie kybernetických incidentov v reálnom čase.

Rozhovor zároveň poukazuje na rastúci význam kybernetickej bezpečnosti v digitálnej spoločnosti a na potrebu spolupráce medzi výskumnými inštitúciami a technologickými firmami pri vývoji nových riešení. Zdôraznená je aj úloha vzdelávania, výskumu a vývoja inovatívnych nástrojov, ktoré pomáhajú organizáciám efektívnejšie reagovať na moderné kybernetické hrozby.

Publikovanie článku na webovej stránke projektu prispieva k šíreniu informácií o aktivitách projektu a podporuje popularizáciu tém kybernetickej bezpečnosti medzi odbornou aj širšou verejnosťou.

Celé znenie článku sa nachádza v prílohe 17 – Článok o rozhovore s odborníkmi Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD.



Obrázok 11: 4.1.1.11 Článok o rozhovore s odborníkmi Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD., Zdroj: (BRAIN:IT, 2025)

1.1.1.12 Článok o rozhovore o projekte INNOSOC: Kybernetická bezpečnosť a rozširovanie obzorov s Dominikou Toman

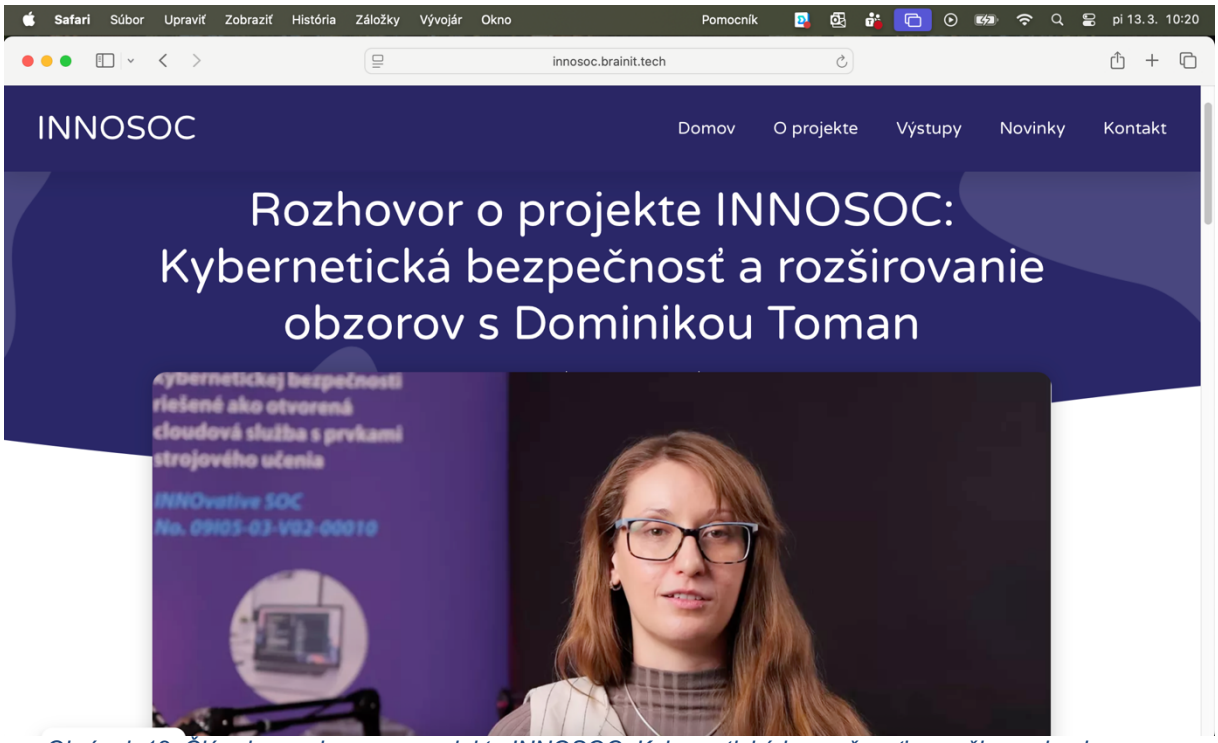
Dňa 11. februára 2026 bol na webovej stránke projektu INNOSOC zverejnený článok predstavujúci rozhovor s **Ing. Dominikou Toman, PhD.**, odbornou asistentkou na Katedre manažérskych teórií Fakulty riadenia a informatiky Žilinskej univerzity v Žiline. Rozhovor približuje jej úlohu v projekte, najmä v oblasti podpory projektového riadenia a koordinácie tímu, a zároveň poukazuje na význam projektu pre odbornú aj širšiu verejnosť.

V článku je zdôraznený prínos projektu INNOSOC v oblasti šírenia poznatkov o kybernetickej bezpečnosti a podpory implementácie moderných bezpečnostných riešení. Projekt sa zameriava na odborné publikovanie výsledkov, prezentovanie výstupov na konferenciách, tvorbu analytických rešerší o vhodných riešeniach pre zvýšenie kybernetickej bezpečnosti a prípravu podkladov pre školenia zamestnancov organizácií.

Rozhovor zároveň poukazuje na význam spolupráce medzi akademickou sférou a odborníkmi z praxe, ktorá umožňuje vytvárať kvalitné a prakticky využiteľné výstupy projektu. Súčasťou článku je aj reflexia osobného a odborného rozvoja členov riešiteľského tímu, ktorí prostredníctvom účasti na projekte získavajú nové poznatky a skúsenosti v oblasti riadenia projektov a kybernetickej bezpečnosti.

Publikovanie článku na webovej stránke projektu prispieva k informovaniu verejnosti o aktivitách projektu a k popularizácii tém kybernetickej bezpečnosti.

Celé znenie článku sa nachádza v prílohe 18 – Článok o rozhovore o projekte INNOSOC: Kybernetická bezpečnosť a rozširovanie obzorov s Dominikou Toman.



Obrázok 12: Článok o rozhovore o projekte INNOSOC: Kybernetická bezpečnosť a rozširovanie obzorov s Dominikou Toman, zdroj: (BRAIN:IT, 2026)

1.1.1.13 Článok o rozhovore o projekte INNOSOC: O vedeckom výskume a kybernetickej bezpečnosti s Martinom Mičiakom

Dňa 12. februára 2026 bol na webovej stránke projektu INNOSOC zverejnený článok prezentujúci rozhovor s Ing. Martinom Mičiakom, PhD., výskumným pracovníkom z Katedry manažérskych teórií Fakulty riadenia a informatiky Žilinskej univerzity v Žiline. V projekte pôsobí ako člen výskumného tímu a zároveň sa podieľa na podpore projektového riadenia.

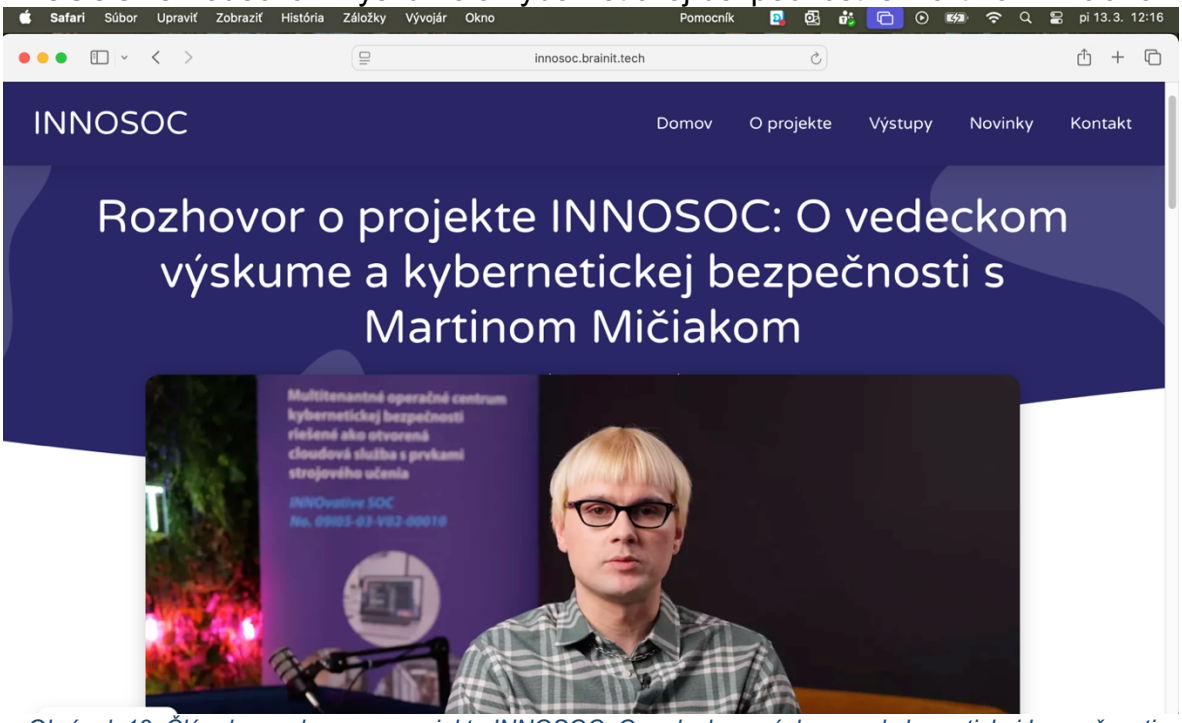
Rozhovor približuje hlavné zameranie projektu INNOSOC v oblasti kybernetickej bezpečnosti a jeho snahu identifikovať a implementovať efektívne riešenia na posilnenie ochrany organizácií pred kybernetickými hrozbami. Osobitná pozornosť je venovaná využívaniu open-source nástrojov, ktoré umožňujú budovať bezpečnostné riešenia s nižšími nákladmi a zároveň zachovať vysokú úroveň ochrany.

Článok zároveň poukazuje na význam kvalitných vedeckých výstupov v rámci projektu, najmä publikovania výsledkov výskumu v renomovaných vedeckých časopisoch, databázach a na odborných konferenciách. Zdôraznená je aj potreba identifikácie tzv. výskumnej medzery (research gap), ktorá umožňuje prinášať nové poznatky a posúvať výskum v oblasti kybernetickej bezpečnosti.

Súčasťou rozhovoru je tiež predstavenie spolupráce medzi akademickými pracoviskami Fakulty riadenia a informatiky Žilinskej univerzity v Žiline, konkrétne medzi Katedrou manažérskych teórií a Katedrou informačných sietí. Táto interdisciplinárna spolupráca prispieva k prepojeniu manažérskeho a technologického pohľadu na kybernetickú bezpečnosť a podporuje tvorbu prakticky využiteľných výstupov projektu.

Publikovanie článku na webovej stránke projektu prispieva k šíreniu informácií o aktivitách projektu a k zvýšeniu povedomia o témach kybernetickej bezpečnosti medzi odbornou aj širšou verejnosťou.

Celé znenie článku sa nachádza v prílohe 19 – Článok o rozhovore o projekte INNOSOC: O vedeckom výskume a kybernetickej bezpečnosti s Martinom Mičiakom.



Obrázok 13: Článok o rozhovore o projekte INNOSOC: O vedeckom výskume a kybernetickej bezpečnosti s Martinom Mičiakom. Zdroj: (BRAIN:IT, 2026)

1.1.1.14 Článok o rozhovore s prof. Ing. Milanom Kubinom, PhD. o projekte INNOSOC

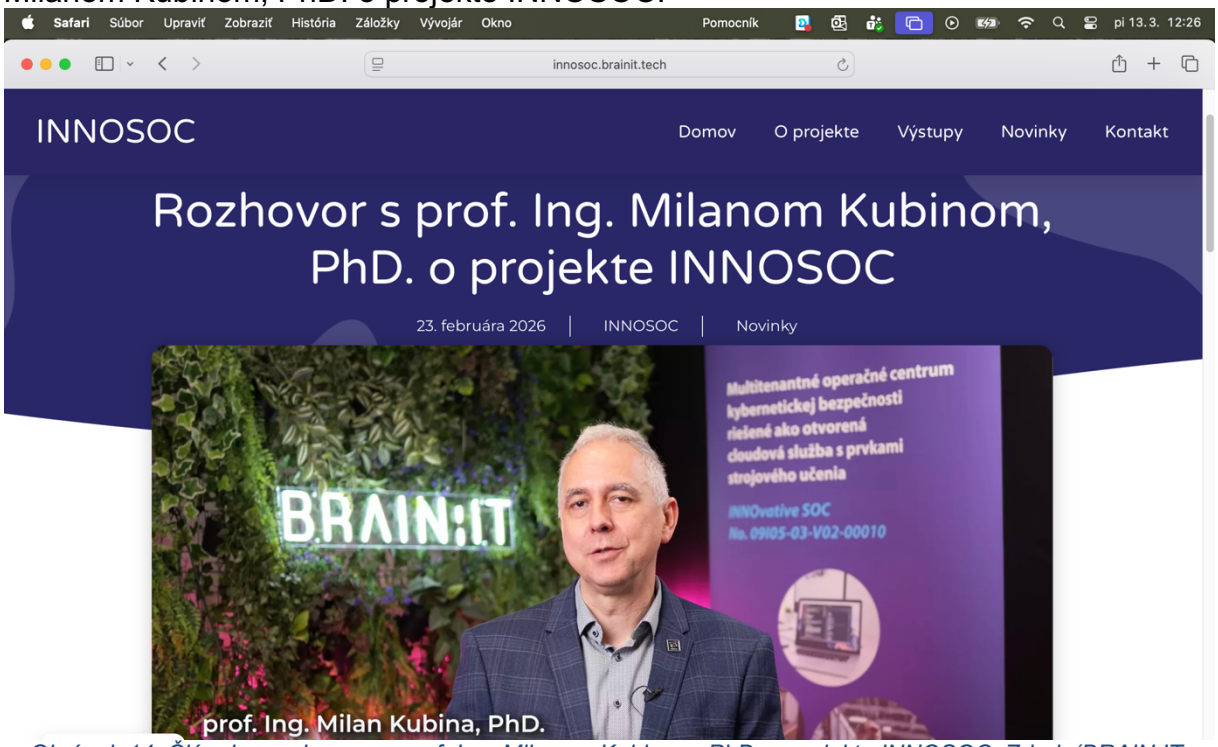
Dňa 23. februára 2026 bol na webovej stránke projektu INNOSOC zverejnený článok prezentujúci odborný rozhovor s prof. Ing. Milanom Kubinom, PhD., ktorý približuje strategické smerovanie projektu a jeho význam v kontexte rastúcich kybernetických hrozieb. V rozhovore je zdôraznené, že projekt reaguje na narastajúce riziká zneužívania systémových zraniteľností v digitálnom prostredí a zameriava sa na vývoj moderných nástrojov podporujúcich ochranu informačných systémov.

Článok predstavuje hlavné ciele projektu, najmä vývoj inovatívnych riešení pre Security Operations Center (SOC) a nástroje na správu IP sietí. Dôraz je kladený na zvyšovanie kybernetickej reziliencie organizácií s obmedzenými rozpočtovými možnosťami, ako sú malé a stredné podniky, orgány verejnej správy či vzdelávacie inštitúcie.

Rozhovor zároveň poukazuje na aktuálny stav vývoja riešenia a zdôrazňuje význam spolupráce medzi akademickou sférou a aplikačnou praxou. Kľúčovú úlohu v projekte zohráva synergia medzi výskumnými pracoviskami a technologickou spoločnosťou BRAIN:IT, ktorá umožňuje prenášať výsledky výskumu do prakticky využiteľných riešení.

Publikovanie článku na webovej stránke projektu prispieva k informovaniu odbornej aj širšej verejnosti o aktivitách projektu a podporuje šírenie poznatkov v oblasti kybernetickej bezpečnosti.

Celé znenie článku sa nachádza v prílohe 20 – Článok o rozhovore s prof. Ing. Milanom Kubinom, PhD. o projekte INNOSOC.



Obrázok 14: Článok o rozhovore s prof. Ing. Milanom Kubinom, PhD. o projekte INNOSOC, Zdroj: (BRAIN:IT, 2026)

1.2 Sociálne siete

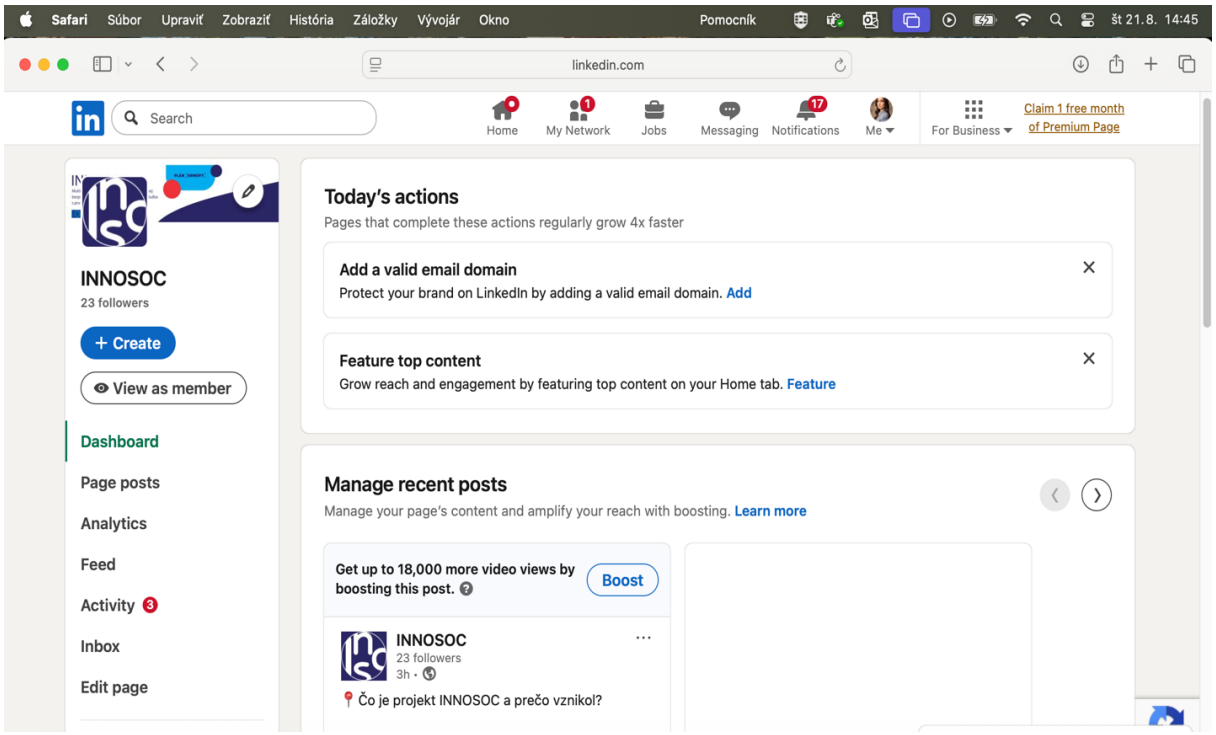
Efektívna komunikácia výstupov projektu je nevyhnutná nielen pre naplnenie jeho odborných a výskumných cieľov, ale aj pre zabezpečenie ich spoločenského a praktického dopadu. Vzhľadom na zameranie projektu INNOSOC – vývoj inovatívneho multitenantného bezpečnostného centra – bola kľúčovým aspektom propagácie cielene orientovaná a dôveryhodná digitálna komunikácia, ktorá osloví správne publikum: od technických odborníkov cez verejnú správu až po mladú generáciu odborníkov a študentov IT odborov.

1.2.1 Realizované aktivity

1.2.1.1 Vytvorenie stránky na sociálnej sieti LinkedIn

Pre komunikáciu a zdieľanie informácií s komunitou profesionálov, medzi ktorých patria výskumníci, odborníci, akademici a iné firmy, bola vytvorená stránka na sociálnej sieti LinkedIn s názvom @INNOSOC. Komunikáciou na tejto sociálnej sieti sa predpokladá efektívne cielenie na odbornú verejnosť. Stránka zároveň komunikuje dlhšie odborné príspevky, články a slúži ako kanál na komunikáciu s odbornou verejnosťou. Povaha tejto sociálnej siete zabezpečila vysokú mieru dôveryhodnosti.

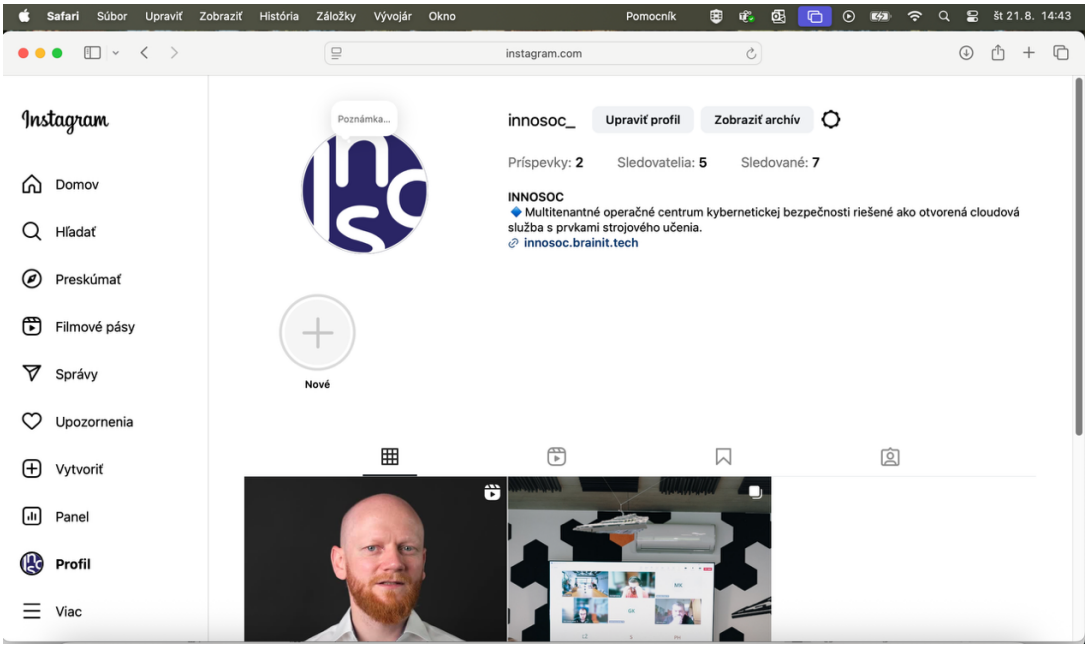
Stránka obsahuje profilovú fotografiu, titulnú fotografiu ktorá zobrazuje logá vykonávateľov. Rovnako tak sa na nej používateľ dozvie o čom projekt je, kto sú partneri projektu a cez odkaz sa dostane na webovú stránku.



Obrázok 15: LinkedIn stránka pre projekt INNOSOC, Zdroj: (BRAIN:IT, 2025)

1.2.1.2 Vytvorenie profilu na sociálnej sieti Instagram

Pre komunikáciu s mladými študentami, mladými profesionálmi a širokou verejnosťou bol vytvorený Instagramový profil s názvom @innosoc_. Instagramový profil bol doplnený o profilovú fotku a o krátky popis projektu, ktorý ho predstaví každému, kto profil navštívi. Profil zároveň obsahuje aj odkaz na webovú stránku.

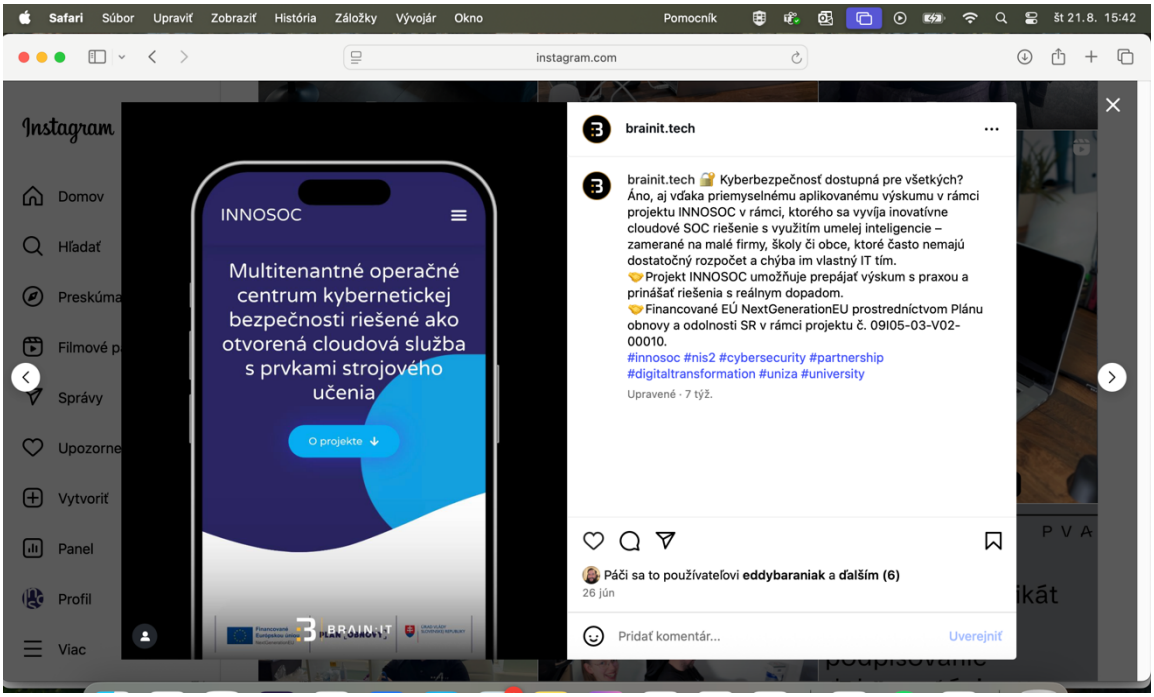


Obrázok 16: Instagramový profil INNOSOC, Zdroj: (BRAIN:IT, 2025)

1.2.1.3 *Príspevok komunikujúci dostupnosť webovej stránky INNOSOC na Instagrame @brainit.tech*

Cieľom príspevku na Instagramovom profile @brainit.tech, ktorý bol zverejnený 26. júna 2025, bolo prvotne komunikovať existenciu projektu INNOSOC ako priemyselného aplikovaného výskumu. Príspevok bol zverejnený na Instagramovom profile partnera projektu BRAIN:IT, ktorý ma veľkú základňu komunity mladých ľudí, medzi ktorými sa nachádzajú študenti stredných a vysokých škôl ako aj mladí odborníci. Príspevok dáva na povedomie aj vytvorenú webovú stránku INNOSOC. Zverejnený obsah obsahoval:

- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.



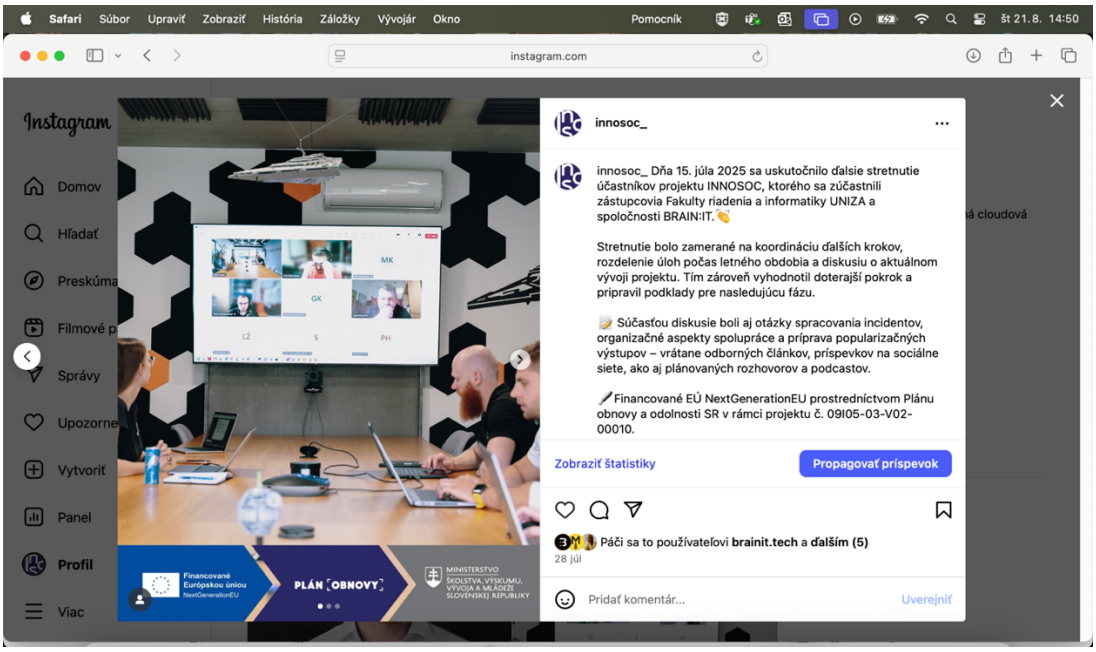
Obrázok 17: Príspevok na Instagramovom účte @brain.tech, Zdroj: (BRAIN:IT, 2025)

1.2.1.4 *Príspevok o stretnutí partnerov 15.7.2025 na Instagrame @innosoc_*

Cieľom príspevku uverejneného dňa 28. júla 2025 bolo komunikovať priebeh stretnutia partnerov projektu, spoločnosti BRAIN:IT a Fakulty riadenia a informatiky, Žilinskej univerzity v Žiliny. Príspevok o stretnutí z 15.júla 2025 komunikuje aktuálny priebeh prác na projekte, ďalšie smerovanie aj organizačné aktivity na nasledujúce obdobie, ktoré sa riešili online stretnutím. Zverejnený obsah obsahoval:

- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.

Publikovaním príspevku na sociálnej sieti Instagram bolo cieľom zaujať a osloviť študentov stredných a vysokých škôl. Publikované príspevky je možné vidieť na obrázku 14.

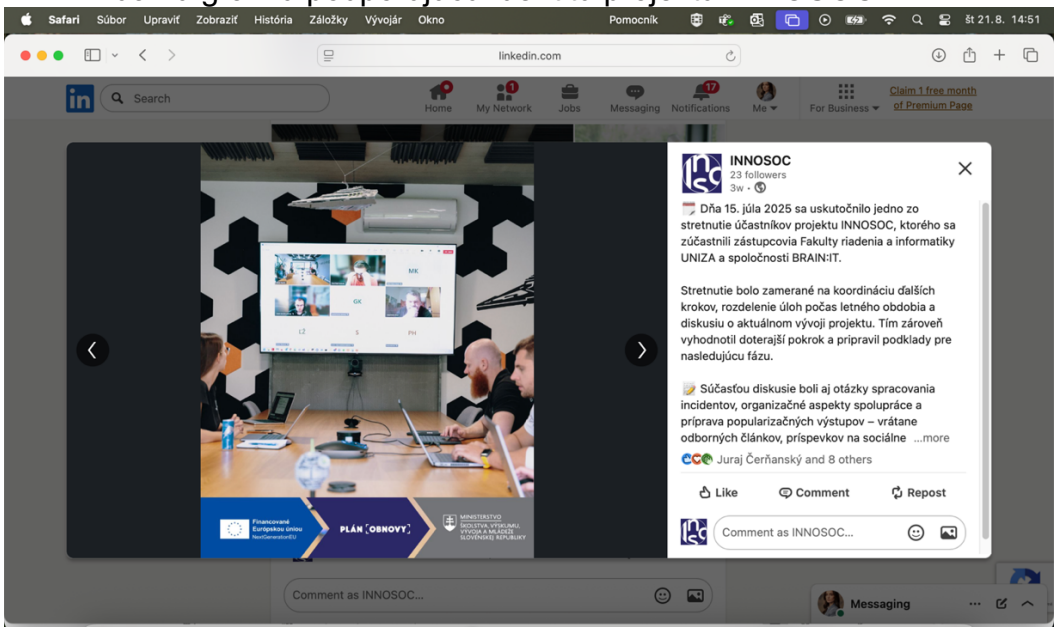


Obrázok 18: Príspevok o stretnutí partnerov 15.7.2025 na Instagrame @innosoc_, Zdroj: (BRAIN:IT, 2025)

1.2.1.5 Príspevok o stretnutí partnerov 15.7.2025 na LinkedIne @INNOSOC

Cieľom príspevku uverejneného dňa 28. júla 2025 bolo komunikovať priebeh stretnutia partnerov projektu, spoločnosti BRAIN:IT a Fakulty riadenia a informatiky, Žilinskej univerzity v Žiline. Príspevok na sociálnej sieti LinkedIn je zameraný na oslovenie odborníkov, výskumníkov a B2B segment. Príspevok o stretnutí z 15.7.2025 komunikuje aktuálny priebeh prác na projekte, ďalšie smerovanie aj organizačné aktivity na nasledujúce obdobie, ktoré sa riešili online stretnutím. Publikovaním na sociálnej sieti LinkedIn sa vytvára odborná diskusia. Zverejnený obsah obsahoval:

- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.



Obrázok 19: Príspevok o stretnutí partnerov 15.7.2025 na LinkedIne @INNOSOC, Zdroj: (BRAIN:IT, 2025)

1.2.1.6 *Príspevok o základných informáciách o projekte INNOSOC na Instagramovom profile @innosoc_ a LinkedIn stránke @INNOSOC z dňa 21.8.2025*

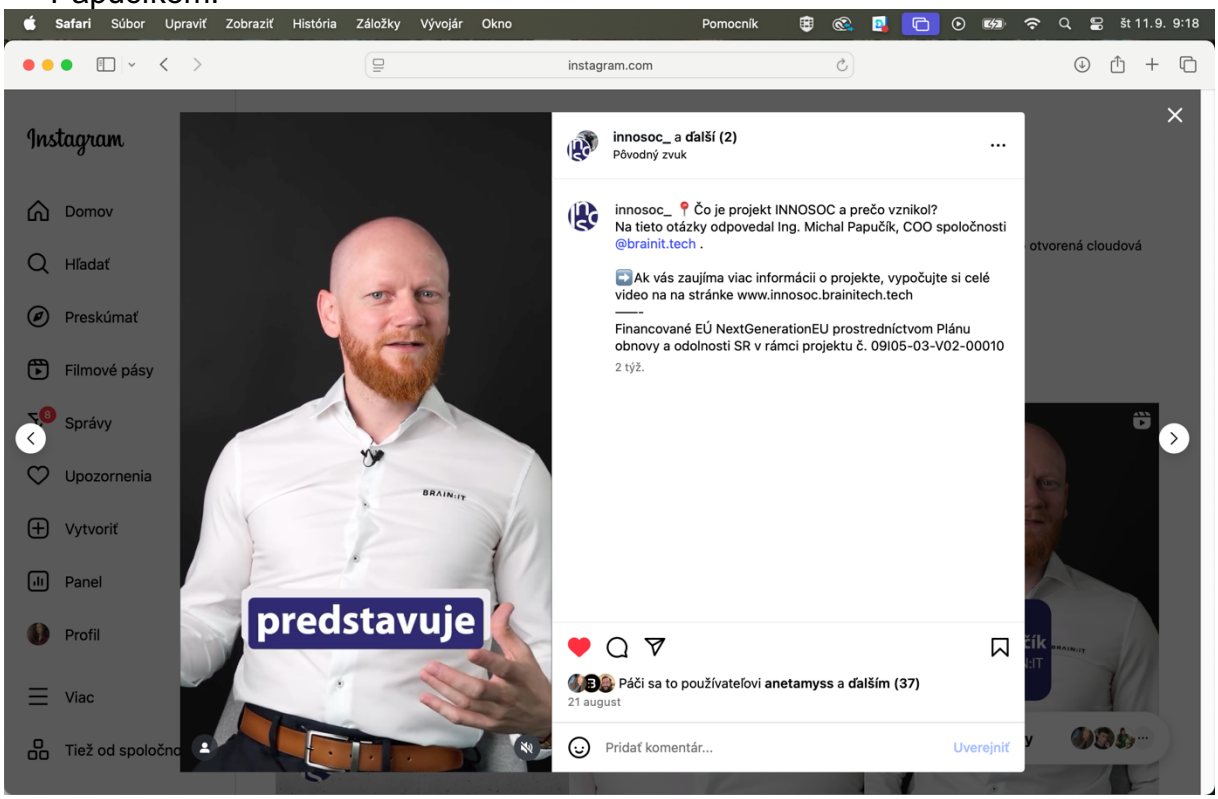
Dňa 21. augusta 2025 bolo zverejnené krátke video na Instagrame @innosoc_ a LinkedIn stránke @INNOSOC. Video obsahuje časť rozhovoru, ktorá bola natočená s Ing. Michalom Papučíkom, a ktorý sa celý nachádza na YouTube kanále @INNOSOC. V tomto krátkom zverejnenom videu sa publikum a široká verejnosť dozvedá základné informácie o projekte ako sú:

- Čo je projekt INNOSOC a prečo vznikol?
- Čo reprezentuje názov INNOSOC?

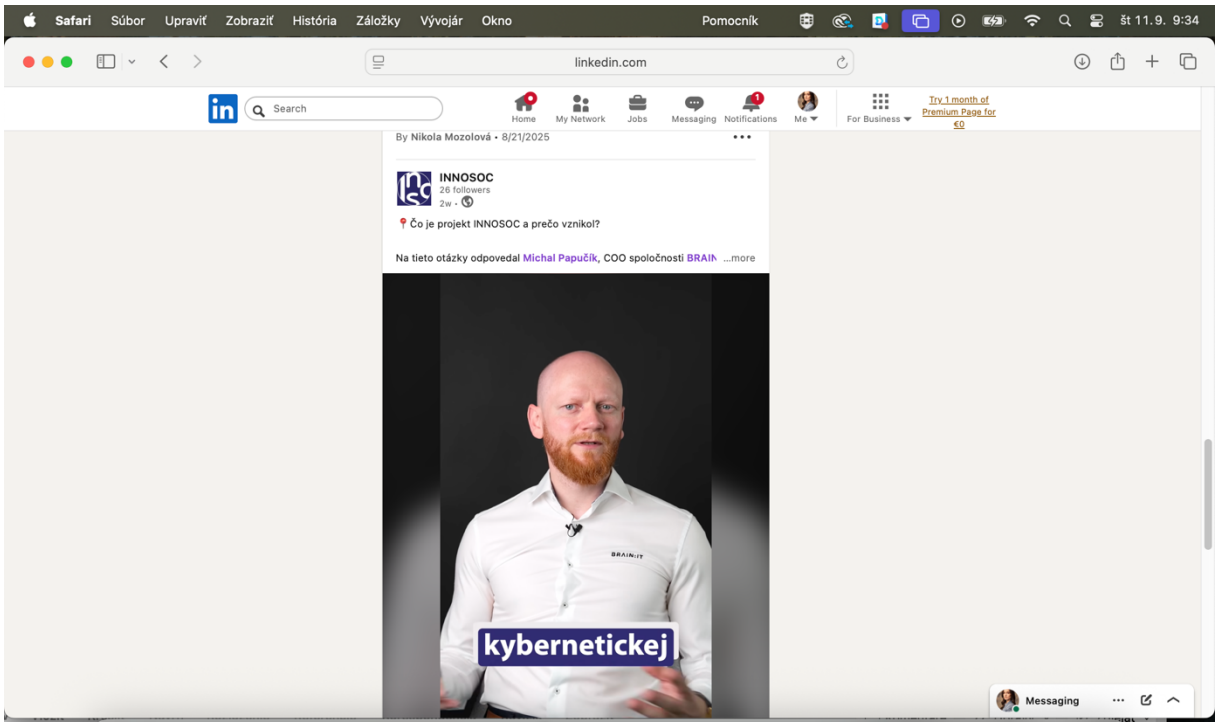
Video má dĺžku 54 sekúnd, čo ho robí atraktívnym pre používateľov sociálnych sieti. Je krátke, výstižne vyjadruje pointu a vďaka doplneným titulkám umožňuje širšie zdieľanie informácií. Cieľom videa je priniesť osvetu o projekte a vysvetliť jeho cieľ a význam širšiemu publiku, študentom a mladým odborníkom atraktívnym spôsobom. Zverejnený obsah obsahoval:

- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.

Prepis celého videa sa nachádza v prílohe 15 – Rozhovor s Ing. Michalom Papučíkom.



Obrázok 20 Príspevok vo forme krátkeho videa na Instagrame @innosoc_ z dňa 21.8.2025, Zdroj: (BRAIN:IT, 2025)



Obrázok 21 Príspevok vo forme krátkeho videa na LinkedIn stránke @INNOSOC z dňa 21.8.2025 , Zdroj: (BRAIN:IT, 2025)

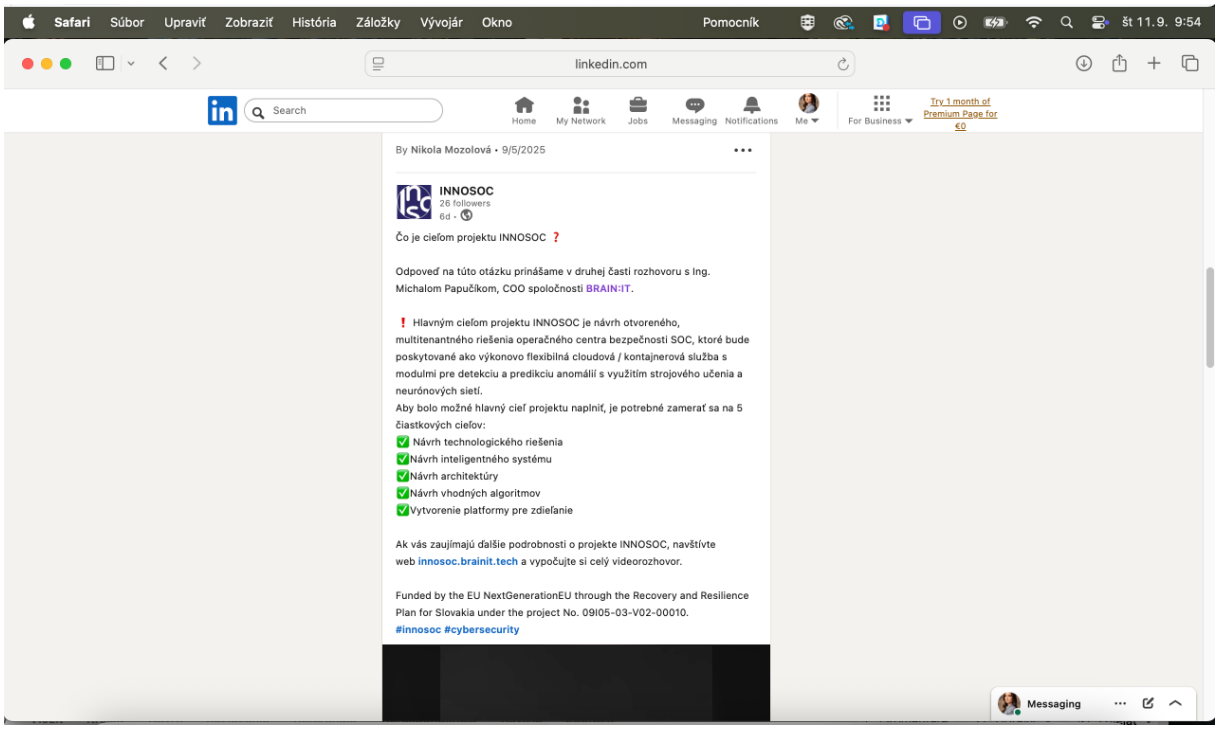
1.2.1.7 Príspevok o základných informáciách o projekte INNOSOC na Instagramovom profile @innosoc_ a LinkedIn stránke @INNOSOC z dňa 5.9.2025

Dňa 5.septembra.2025 bol zverejnený príspevok vo forme krátkeho videa. Video má 31 sekúnd a obsahuje časť rozhovoru s Ing. Michalom Papučíkom, ktorý je celý zverejnený na YouTube kanále @INNOSOC. Video obsahuje stručné vysvetlenie cieľa projektu. Video je spracované do formátu atraktívneho na sociálne siete tak, aby zaujalo širokú verejnosť, študentov aj mladých odborníkov.

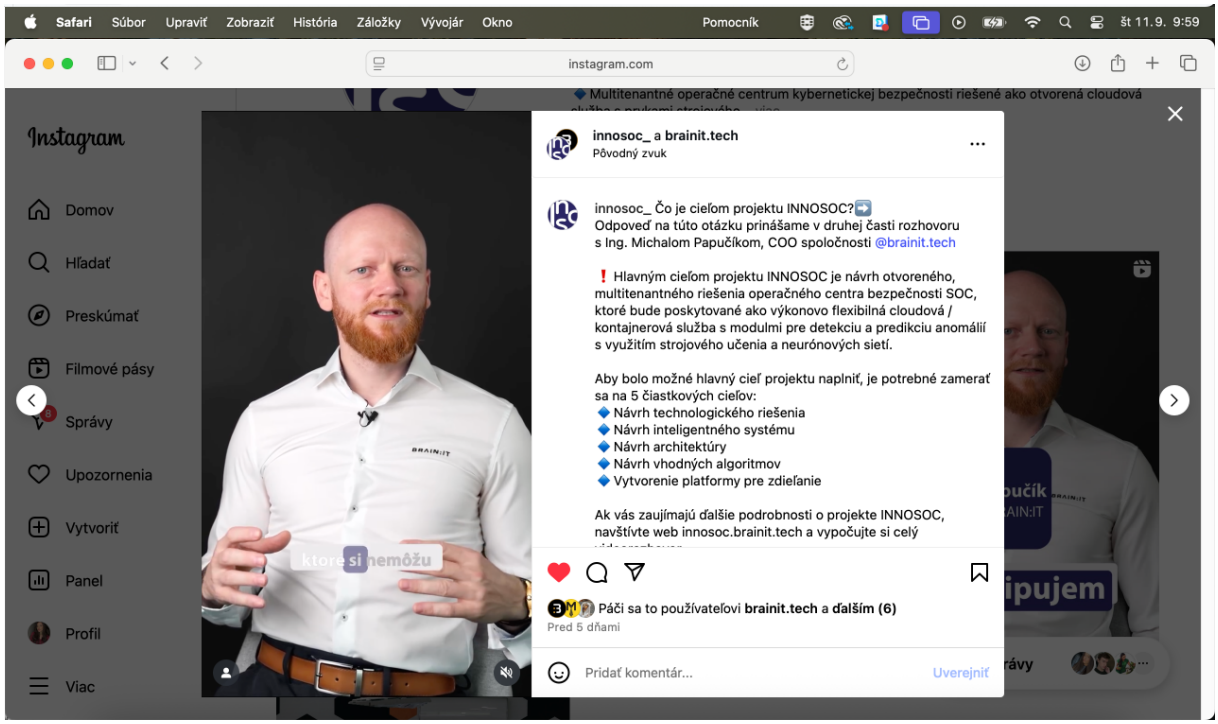
Prostredníctvom príspevku zverejneného na Instagrame @innosoc_ cieli na študentov stredných škôl a mladých odborníkov, zatiaľ čo na LinkedIn stránke @INNOSOC cieli na študentov vysokých škôl, mladých odborníkov a odbornú verejnosť. Zverejnený obsah obsahoval:

- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.

Prepis celého videa sa nachádza v prílohe 15 – Rozhovor s Ing. Michalom Papučíkom.



Obrázok 22 Príspevok vo forme krátkeho videa zverejnený dňa 5.9.2025 na LinkedIne @INNOSOC , Zdroj: (BRAIN:IT, 2025)

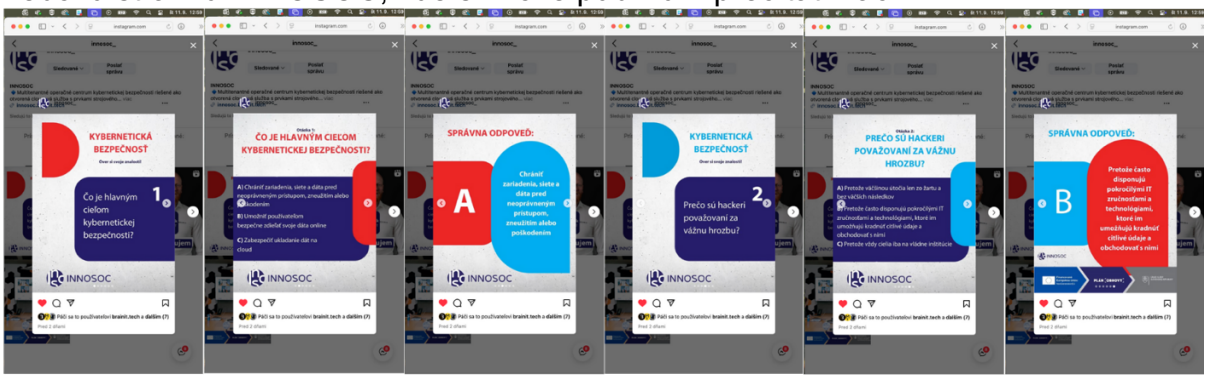


Obrázok 23 Príspevok vo forme krátkeho videa zverejnený dňa 5.9.2025 na Instagrame @innosoc_ , Zdroj: (BRAIN:IT, 2025)

1.2.1.8 Príspevok vo forme kvízu na tému kybernetická bezpečnosť zverejnený dňa 8.septembra 2025

V rámci vzdelávania v oblasti kybernetickej bezpečnosti bol dňa 8.septembra 2025 publikovaný príspevok na Instagram @innosoc_ vo forme série obrázkov. V príspevku sú zakomponované otázky a možnosti týkajúce sa kybernetickej bezpečnosti a hrozieb. Séria obrázkov ponúka výber z možnosti a publikum tak má

možnosť porozmýšľať a vybrať správnu odpoveď, ktorú si môže v príspevku zároveň overiť. Cieľom príspevku je vzdelávať a šíriť osvetu o hrozbách v kybernetickom svete. Otázky v kvíze nadväzujú na popularizačný článok zverejnený na LinkedIn stránke @INNOSOC a na webovej stránke INNOSOC a príspevok zároveň odkazuje aj na webovú stránku INNOSOC, kde si môže publikum prečítať viac.



Obrázok 24 Príspevok vo forme kvízu na tému kybernetická bezpečnosť zverejnený dňa 9.9.2025 na Instagrame @innosoc_, Zdroj: (BRAIN:IT, 2025)

1.2.1.9 Príspevok vo forme kvízu na tému kybernetická bezpečnosť zverejnený dňa 16.septembra 2025

V rámci vzdelávania v oblasti kybernetickej bezpečnosti bol dňa 16.septembra 2025 publikovaný príspevok na Instagram @innosoc_ vo forme série obrázkov. V príspevku sú zakomponované otázky a možnosti týkajúce sa kybernetickej bezpečnosti a hrozieb. Séria obrázkov ponúka výber z možnosti a publikum tak má možnosť porozmýšľať a vybrať správnu odpoveď. Cieľom príspevku je vzdelávať a šíriť osvetu o hrozbách v kybernetickom svete. Otázky v kvíze nadväzujú na popularizačný článok zverejnený na LinkedIn stránke @INNOSOC a na webovej stránke INNOSOC a príspevok zároveň odkazuje aj na webovú stránku INNOSOC, kde si môže publikum prečítať viac.



Obrázok 25: Príspevok na instagramovom účte @innosoc_: kvíz o kybernetickeh bezpečnosti, Zdroj: (BRAIN:IT, 2025)

*1.2.1.10 Informatívny príspevok o prebiehajúcej súťaži o iPad na instagramovom účte @innosoc_*

Dňa 3. októbra 2025 bol na instagramovom účte @innosoc_ zverejnený príspevok, ktorý komunikuje možnosť vyhrať iPad. Cieľom príspevku je zvýšiť záujem mladých o problematiku kybernetickej bezpečnosti. Každý súťažiaci musel pre zapojenie sa do súťaže splniť nasledovné podmienky, ktoré boli uvedené v popise súťažného príspevku:

1. Zapojený musel správne odpovedať na otázku z oblasti kybernetickej bezpečnosti, ktorá bola komunikovaná vo vizuále príspevku aj v popise príspevku.

Znenie súťažnej otázky: „Čo je hlavnou výhodou dvojfaktorovej autentifikácie (2FA)?“

Možnosti odpovede:

a) Zrýchľuje prihlásenie do systémov.
b) Pridáva ďalšiu vrstvu ochrany, takže aj keď je heslo odcudzené, útočník potrebuje ešte ďalší overovací prvok
c) Automaticky generuje nové heslo každý deň pre dodatočnú ochranu.

2. Zapojený musel sledovať 4 instagramové profily, a to @brainit.tech, @budmanazer, @budfri.sk a @innosoc_.
3. Zapojený musel v komentári označiť 1 ďalšiu osobu.

Zverejnený obsah obsahoval:

- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.



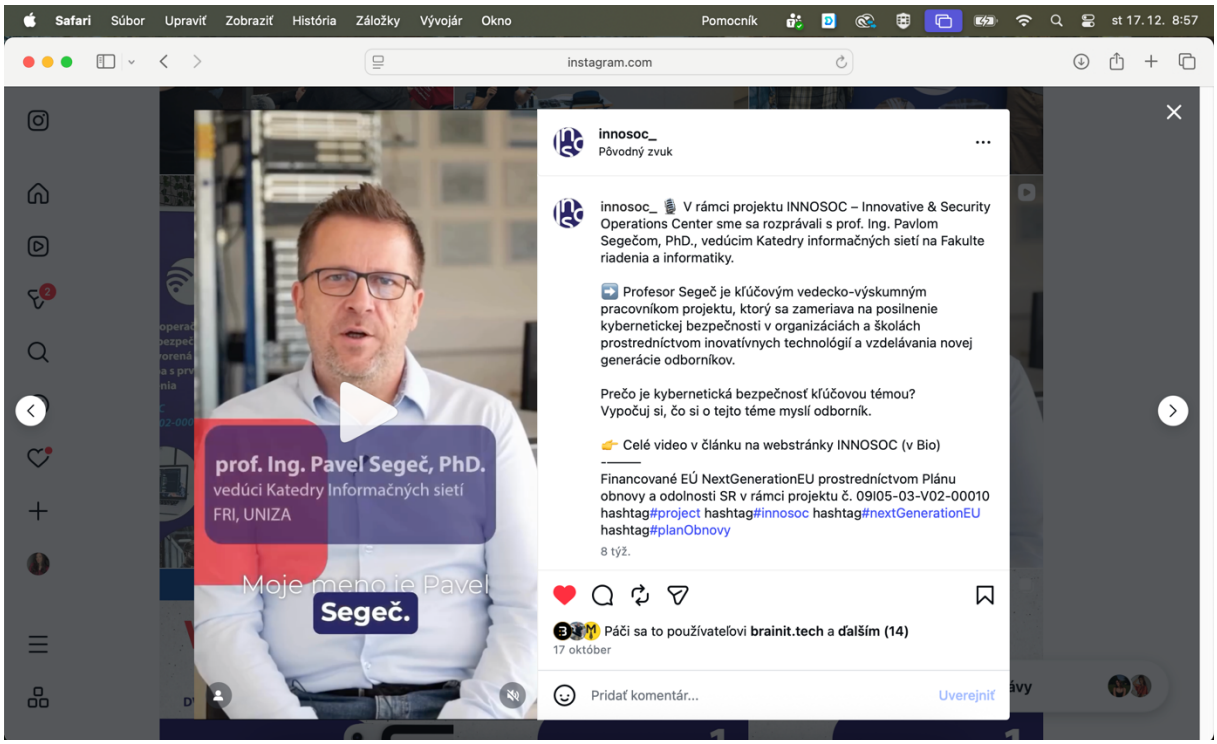
Obrázok 26: príspevok na instagramovom účte @innosoc_: súťaž o iPad, Zdroj: (BRAIN:IT, 2025)

1.2.1.11 Krátke video – rozhovor s prof. Ing. Pavel Segeč, PhD.

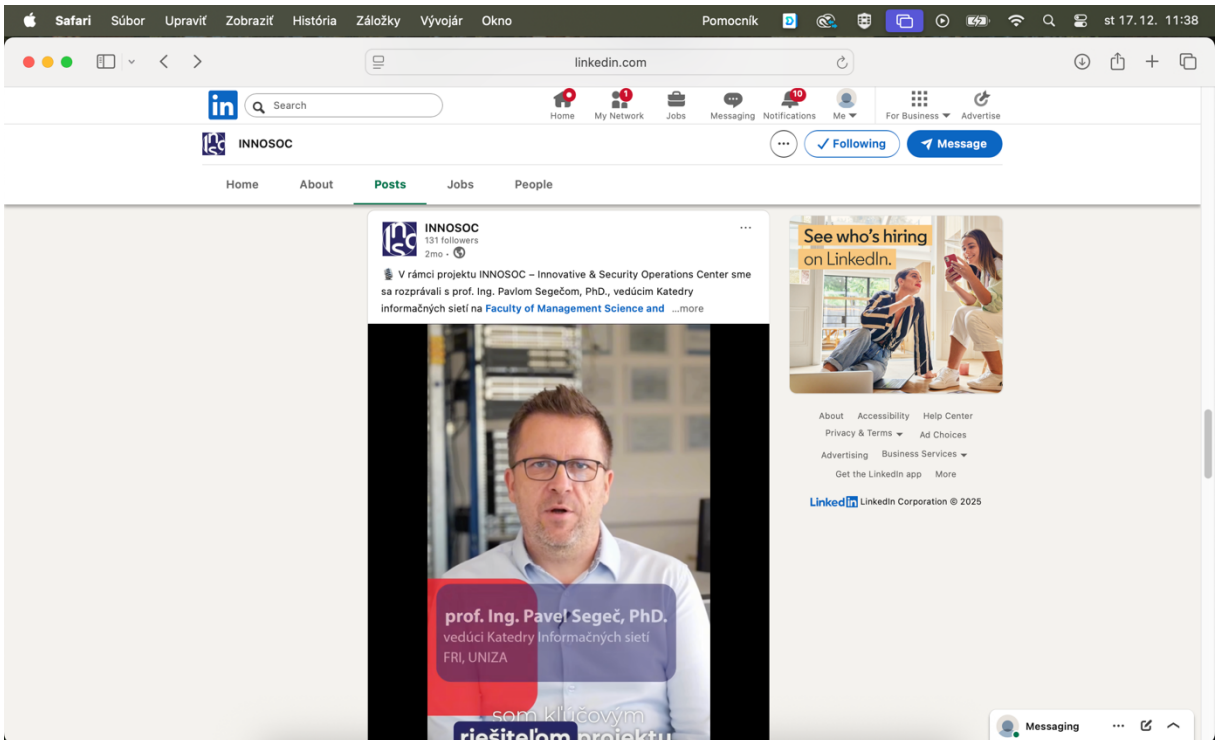
Dňa 17. októbra 2025 bolo na instagramovom účte @innosoc_ a LinkedIn účte @innosoc zverejnené krátke informačné video, ako výstrižok z rozhovoru s prof. Ing. Pavel Segeč, PhD., ktorý na projkete pracuje ako vedecko-výskumný pracovník. Celý rozhovor je v celej dĺžke zverejnený na Youtube kanále INNOSOC. Krátke informačné video komunikuje, prečo je kybernetická bezpečnosť kľúčovou témou. Krátke video má dĺžku 1:02 minúty a je spracované do podoby atraktívnej pre sociálne siete aj s vhodnými titulkami. Zverejnený obsah obsahoval:

- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.

Celý prepis rozhovoru sa nachádza v prílohe 16 – Rozhovor s prof. Ing. Pavlom Segečom, PhD.



Obrázok 27: Krátke video na instagramovom účte @innosoc_, Zdroj: (BRAIN:IT, 2025)



Obrázok 28: krátke video na LinkedIn profile @innosoc: Rozhovor s prof. Ing. Pavel Segeč, PhD., Zdroj: (BRAIN:IT, 2025)

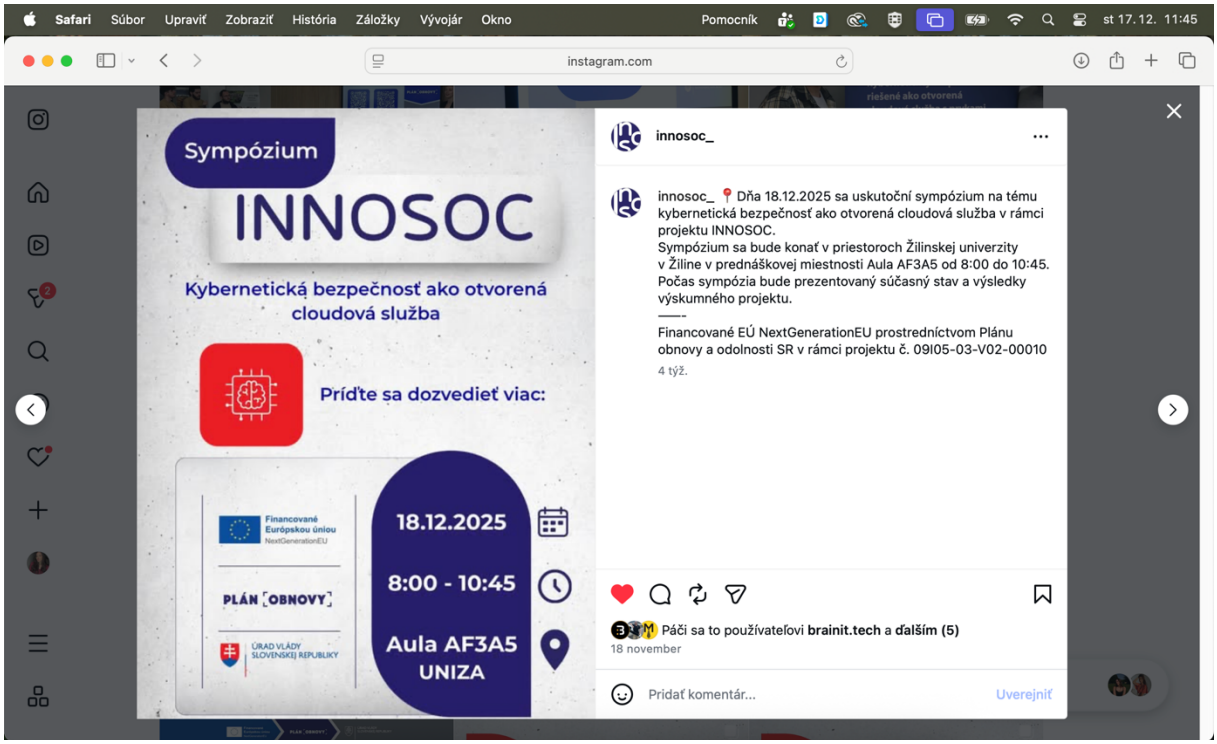
1.2.1.12 Informačný príspevok o konaní sympózia projektu INNOSOC

Dňa 18. novembra 2025 bol zverejnený informačný a pozývací príspevok k odbornému sympóziu na tému „Kybernetická bezpečnosť ako otvorená cloudová služba“ na instagramovom účte @nnosoc_ a LinkedIn účte @innosoc.

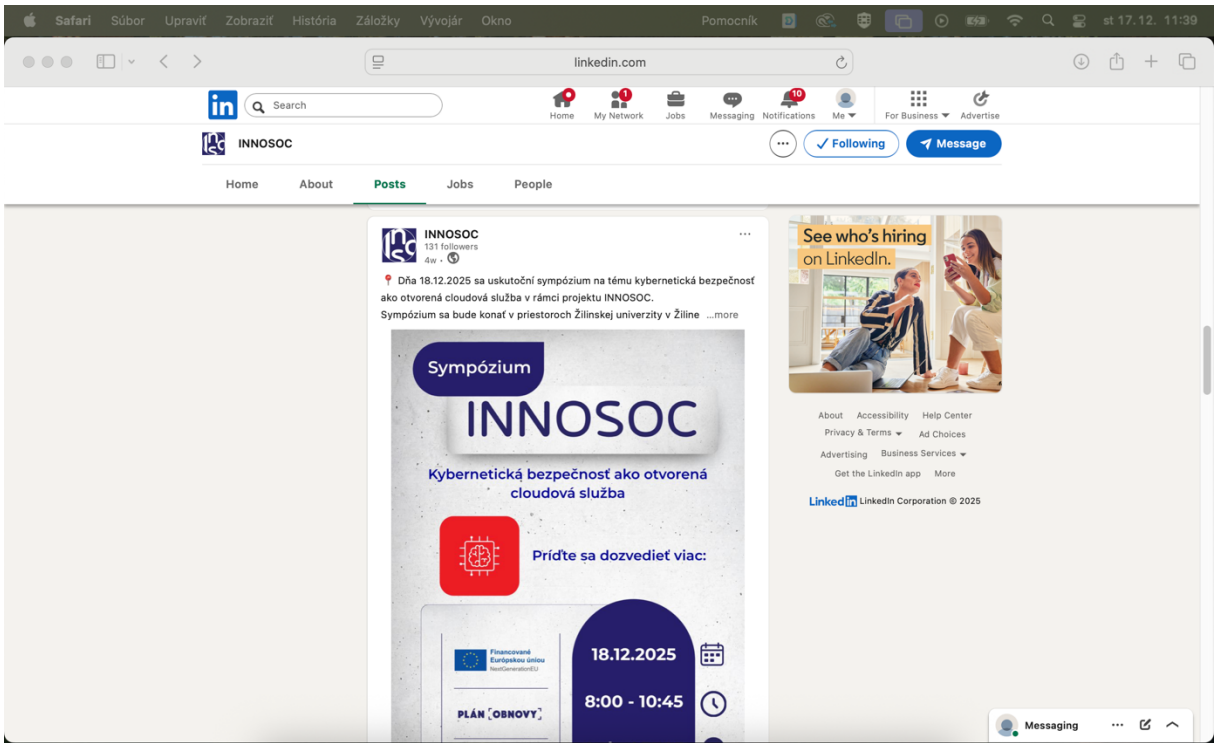
Cieľom príspevku bolo informovať verejnosť, najmä študentov, odbornú a akademickú komunitu, o konaní sympózia, jeho téme, mieste a čase realizácie, ako aj o jeho prepojení na výskumný projekt INNOSOC. Príspevok zároveň slúžil na podporu účasti na podujatí a na šírenie povedomia o aktivitách a výstupoch projektu prostredníctvom sociálnych sietí.Zverejnený obsah obsahoval:

- základné informácie o sympóziu (dátum, čas, miesto konania),
- tematické zameranie sympózia v oblasti kybernetickej bezpečnosti a cloudových služieb,
- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR,
- vizuálnu grafiku podporujúcu identitu projektu INNOSOC.

Príspevok predstavuje diseminačný a popularizačný výstup projektu, zameraný na komunikáciu výsledkov a aktivít projektu INNOSOC v online priestore a na zvýšenie jeho viditeľnosti medzi cieľovými skupinami.



Obrázok 29: Príspevok na instagramovom účte @innosoc_: oznam o konaní sympózia, Zdroj: (BRAIN:IT, 2025)



Obrázok 30: príspevok na LinkedIn profile @innosoc: oznam o konaní sympózia, Zdroj: (BRAIN:IT, 2025)

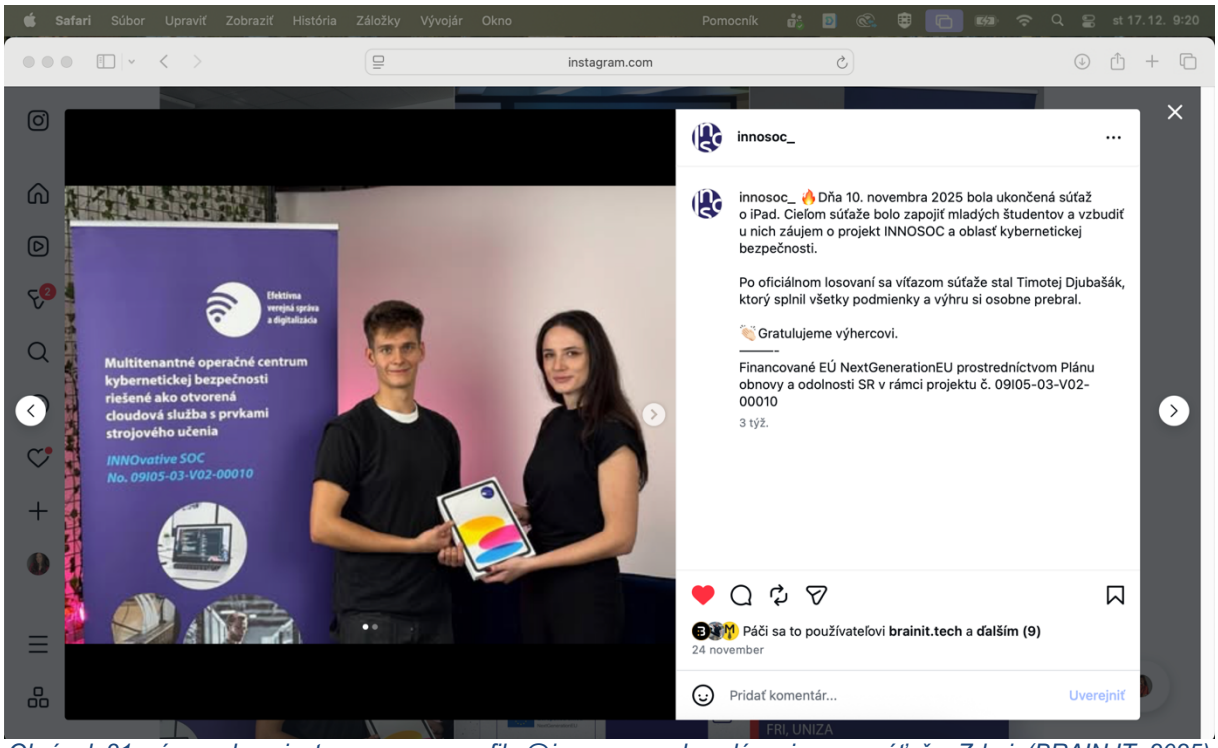
1.2.1.13 Príspevok o ukončení súťaže o iPad

Dňa 24. novembra 2025 bol na instagramovom účte @innosoc_ zverejnený príspevok informujúci o **ukončení študentskej súťaže o iPad** a o jej víťazovi.

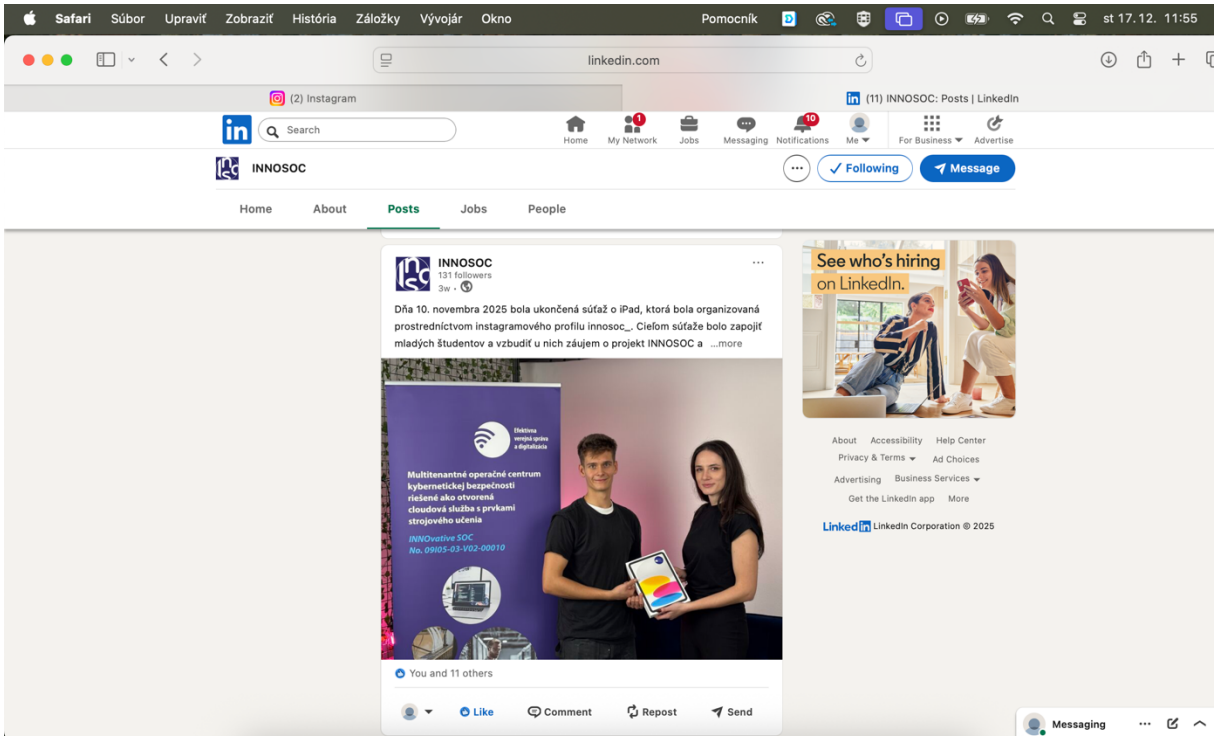
Cieľom príspevku bolo podporiť zapojenie mladých študentov do aktivít projektu INNOSOC, zvýšiť ich záujem o tému kybernetickej bezpečnosti a posilniť povedomie o projekte prostredníctvom interaktívnej formy komunikácie na sociálnych sieťach. Zverejnený obsah zahŕňal:

- informáciu o ukončení súťaže a jej zameraní na podporu záujmu o kybernetickú bezpečnosť,
- oznámenie víťaza súťaže a prezentáciu slávnostného odovzdania výhry,
- vizuálny materiál dokumentujúci realizáciu aktivity,
- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR.

Príspevok predstavuje **diseminačný a popularizačný výstup projektu**, ktorý prispel k zviditeľneniu projektu INNOSOC medzi študentskou verejnosťou, podporil interakciu s cieľovou skupinou a zvýšil atraktivitu projektu prostredníctvom edukačno-motivačných aktivít.



Obrázok 31:príspevok na instagramovom profile @innosoc_: odovzdávanie ceny súťaže, Zdroj: (BRAIN:IT, 2025)



Obrázok 32: prípevok na LinkedIn profile @innosoc_: odovzdávanie ceny súťaže, Zdroj: (BRAIN:IT, 2025)

1.2.1.14 Príspevok o prezentácii projektu INNOSOC na študentských raňajkách

Dňa 28. novembra 2025 bol zverejnený príspevok na instagramovom profile @innosoc_ informujúci o študentských raňajkách, ktoré sa konali dňa 4. novembra 2025 na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline v spolupráci so spoločnosťou BRAIN:IT.

Cieľom príspevku bolo informovať študentov o neformálnej prezentačnej aktivite projektu, zvýšiť povedomie o projekte INNOSOC medzi mladými ľuďmi a priblížiť im aktuálny stav, výstupy a ďalšie smerovanie projektu v oblasti kybernetickej bezpečnosti. Zverejnený obsah zahŕňal:

- informáciu o realizácii študentskej akcie a jej neformálnom charaktere,
- prezentáciu projektu INNOSOC študentom manažérskych a informatických odborov,
- komunikáciu významu kybernetickej bezpečnosti, Security Operations Center a cloudových technológií,
- vizuálnu dokumentáciu podujatia podporujúcu viditeľnosť projektu,
- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR.

Príspevok predstavuje diseminačný, popularizačný a náborový výstup projektu, zameraný na oslovenie študentskej cieľovej skupiny, podporu záujmu o tému kybernetickej bezpečnosti a posilnenie prepojenia medzi výskumným projektom, akademickým prostredím a praxou.



Obrázok 33:príspevok na instagramovom účte @innosoc_: prezentácia na študentských raňajkách, Zdroj: (BRAIN:IT, 2025)

1.2.1.15 Príspevok o prezentácii projektu INNOSOC na Univerzite Tomáše Báti v Zlíne

Dňa 10. decembra 2025 zverejnený príspevok informujúci o prezentácii projektu INNOSOC študentom Fakulty aplikovanej informatiky Univerzity Tomáša Baťu v Zlíne, ktorá sa uskutočnila dňa 20. novembra 2025.

Cieľom príspevku bolo informovať o realizácii prezentačnej aktivity projektu v akademickom prostredí, zvýšiť povedomie o projekte INNOSOC medzi študentmi informačno-technologických odborov a priblížiť im význam kybernetickej bezpečnosti v kontexte digitálnej transformácie. Zverejnený obsah zahŕňal:

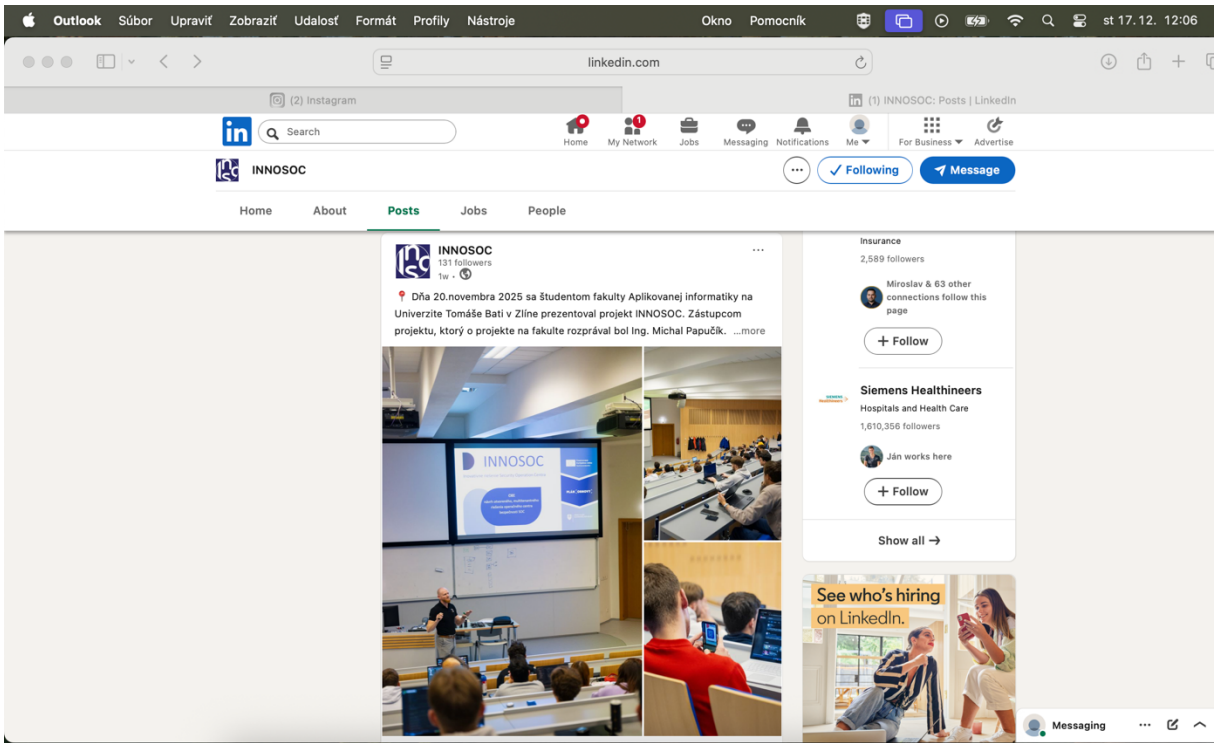
- informáciu o prezentácii projektu študentom aplikovanej informatiky,

- predstavenie cieľov, zamerania a prínosov projektu INNOSOC,
- vysvetlenie významu Security Operations Center a moderných IT bezpečnostných služieb,
- poukázanie na potrebu IT špecialistov a rastúci dopyt po odborníkoch v oblasti kybernetickej bezpečnosti,
- prezentáciu princípov a technológií využívaných v projekte,
- vizuálnu dokumentáciu z prednášky,
- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR.

Príspevok predstavuje diseminačný, prezentačný a popularizačný výstup projektu, ktorý podporuje prepojenie výskumného projektu s akademickou obcou, prispieva k šíreniu výsledkov projektu a motivuje študentov k záujmu o oblasť kybernetickej bezpečnosti a moderných IT riešení.



Obrázok 34: príspevok na instagramovom profile @innosoc_: prezentácia na Univerzite Tomáše Báti v Zlíne, Zdroj: (BRAIN:IT, 2025)



Obrázok 35:príspevok na LinkedIn profile @innosoc: prezentácia na Univerzite Tomáše Báti v Zlíne, Zdroj: (BRAIN:IT, 2025)

1.2.1.16 Príspevok o prezentácii projektu INNNOSC na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici

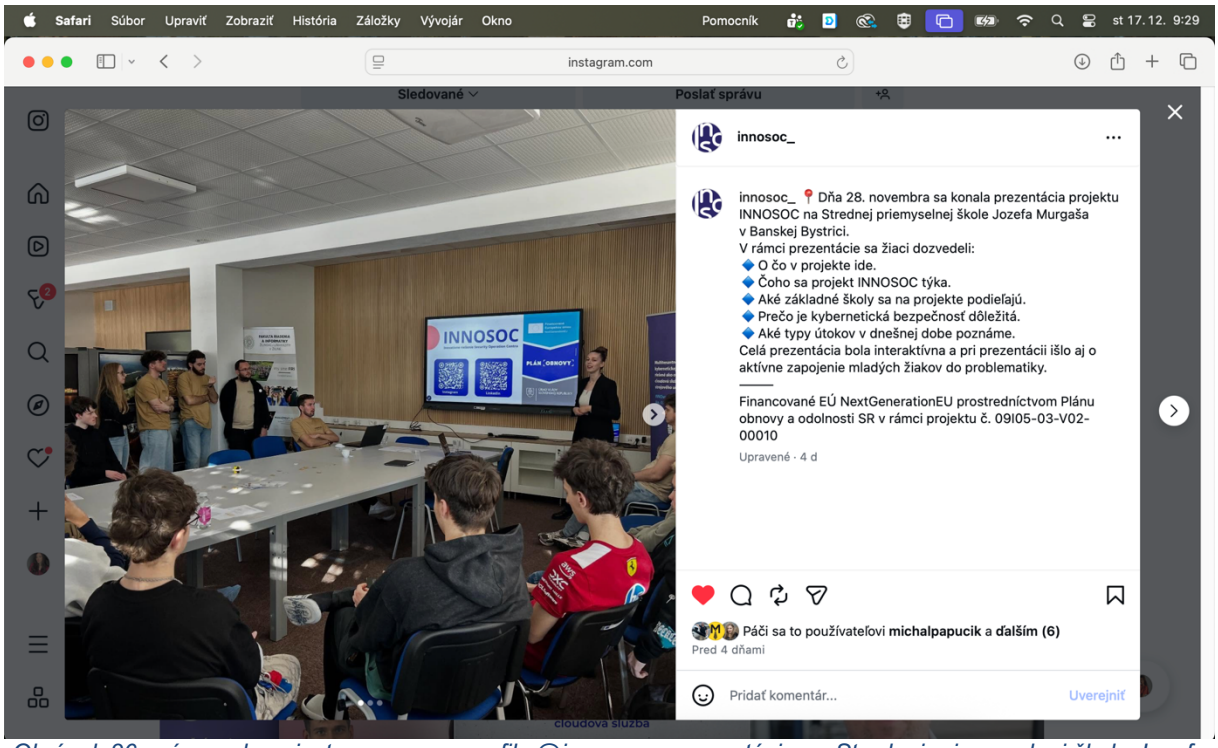
Dňa 12. decembra 2025 bol zverejnený príspevok informujúci o prezentácii projektu INNOSOC na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici, ktorá sa uskutočnila dňa 28. novembra 2025.

Cieľom príspevku bolo informovať verejnosť o realizácii edukačnej aktivity zameranej na zvýšenie povedomia o kybernetickej bezpečnosti medzi žiakmi stredných škôl a priblížiť im význam projektu INNOSOC v kontexte ochrany digitálneho priestoru. Zverejnený obsah zahŕňal:

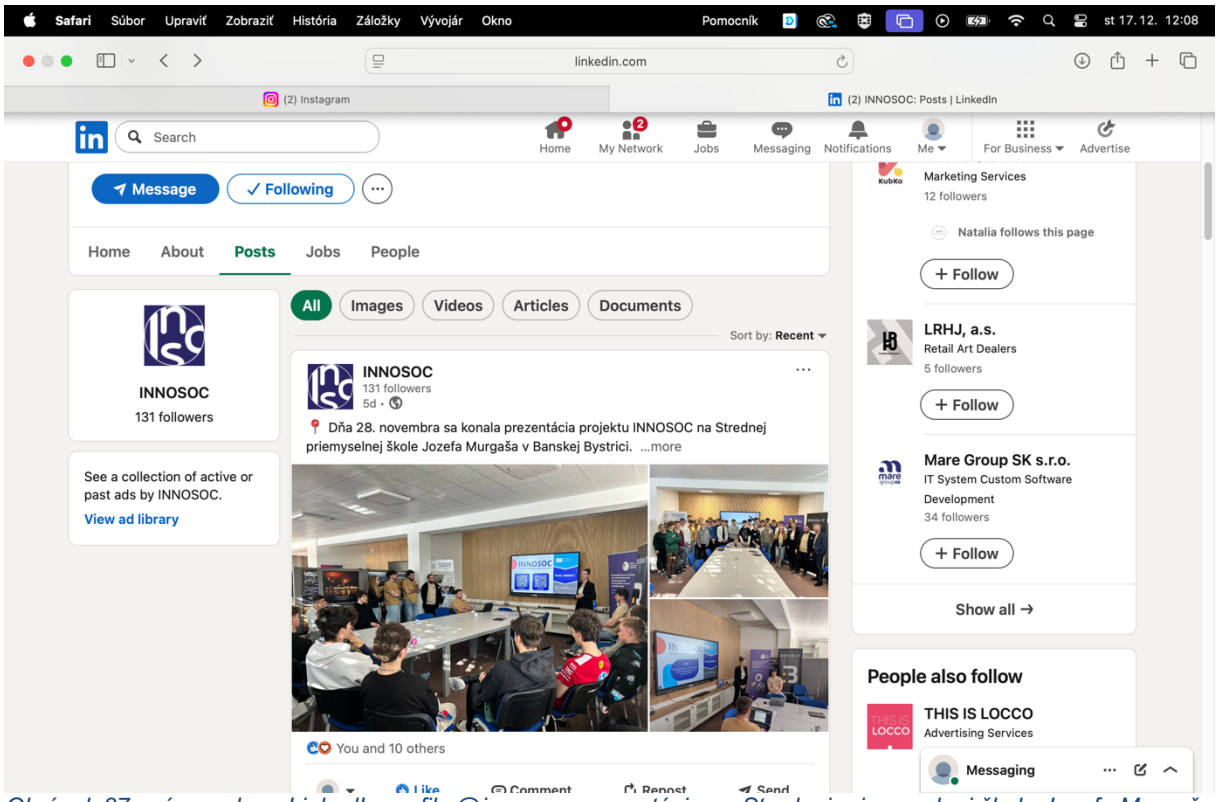
- informáciu o realizácii prezentácie projektu na strednej škole,
- predstavenie cieľov a zamerania projektu INNOSOC,
- vysvetlenie významu kybernetickej bezpečnosti a aktuálnych typov kybernetických útokov,
- prezentáciu zapojených vysokých škôl a partnerov projektu,
- interaktívny charakter prezentácie s aktívnym zapojením žiakov,
- vizuálnu dokumentáciu z edukačnej aktivity,
- informáciu o financovaní projektu z prostriedkov EÚ – NextGenerationEU v rámci Plánu obnovy a odolnosti SR.

Príspevok predstavuje diseminačný, edukačný a popularizačný výstup projektu, zameraný na oslovenie mladšej cieľovej skupiny, podporu digitálnej gramotnosti a budovanie povedomia o dôležitosti kybernetickej bezpečnosti už na úrovni stredného vzdelávania.

Celé znenie článku sa nachádza v prílohe 9 – Článok o prezentácii projektu INNOSOC na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici.



Obrázok 36: príspevok na instagramovom profile @innosoc_: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici, Zdroj: (BRAIN:IT, 2025)



Obrázok 37: príspevok na LinkedIn profile @innosoc: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici, Zdroj: (BRAIN:IT, 2025)

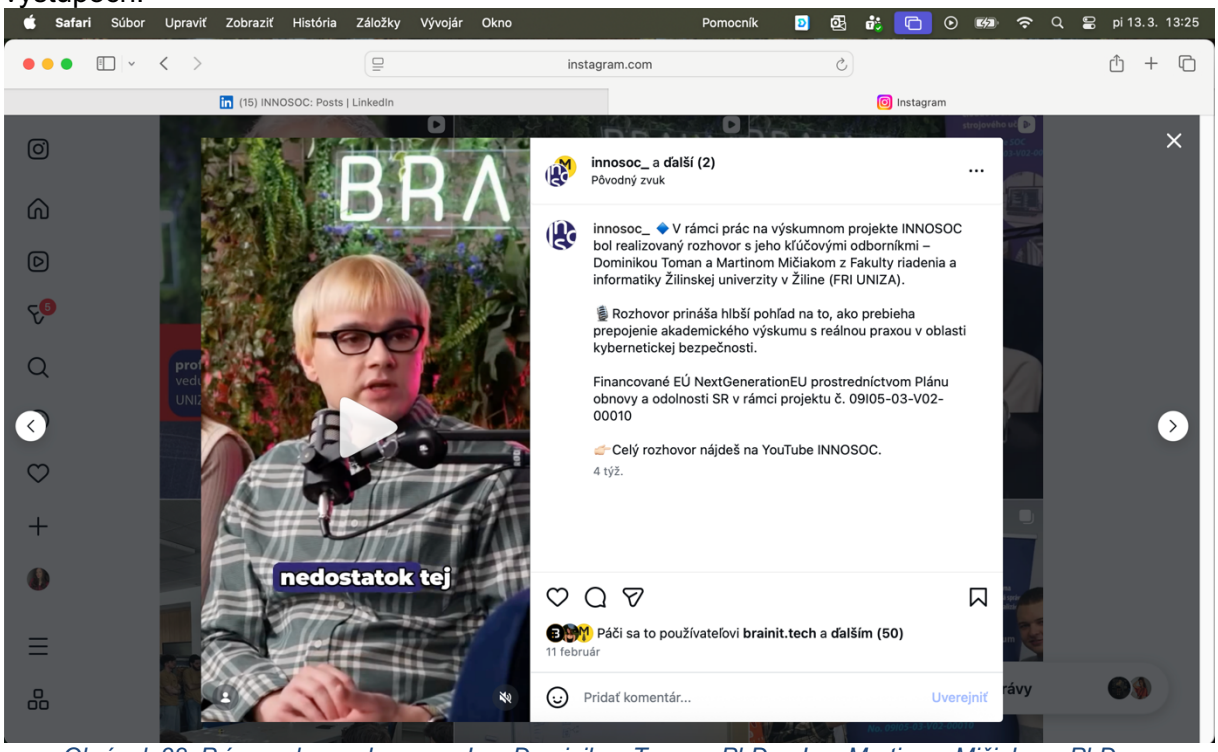
1.2.1.17 Krátke video – rozhovor s Ing. Martinom Mičiakom, PhD.

Dňa 11. februára 2026 bol v rámci komunikačných a popularizačných aktivít projektu INNOSOC na instagramovom profile @innosoc_ zverejnený príspevok informujúci o

realizovanom rozhovore s odborníkmi zapojenými do projektu – Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD. z Fakulty riadenia a informatiky Žilinskej univerzity v Žiline. Príspevok upozorňoval na dostupnosť video-rozhovoru publikovaného na platforme YouTube v rámci kanála projektu INNOSOC.

Obsah rozhovoru približuje fungovanie projektu a poskytuje hlbší pohľad na prepojenie akademického výskumu s praktickými potrebami v oblasti kybernetickej bezpečnosti. Diskusia sa zameriava najmä na význam spolupráce medzi univerzitným prostredím a odborníkmi z praxe, ktorá umožňuje vytvárať inovatívne riešenia a zároveň zabezpečuje praktickú využiteľnosť výstupov projektu.

Príspevok zároveň informoval o financovaní projektu z prostriedkov Európskej únie – NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR, v rámci projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia“ (kód projektu 09I05-03-V02-00010). Zverejnenie príspevku prispelo k informovaniu verejnosti o aktivitách projektu a k šíreniu povedomia o jeho výstupoch.



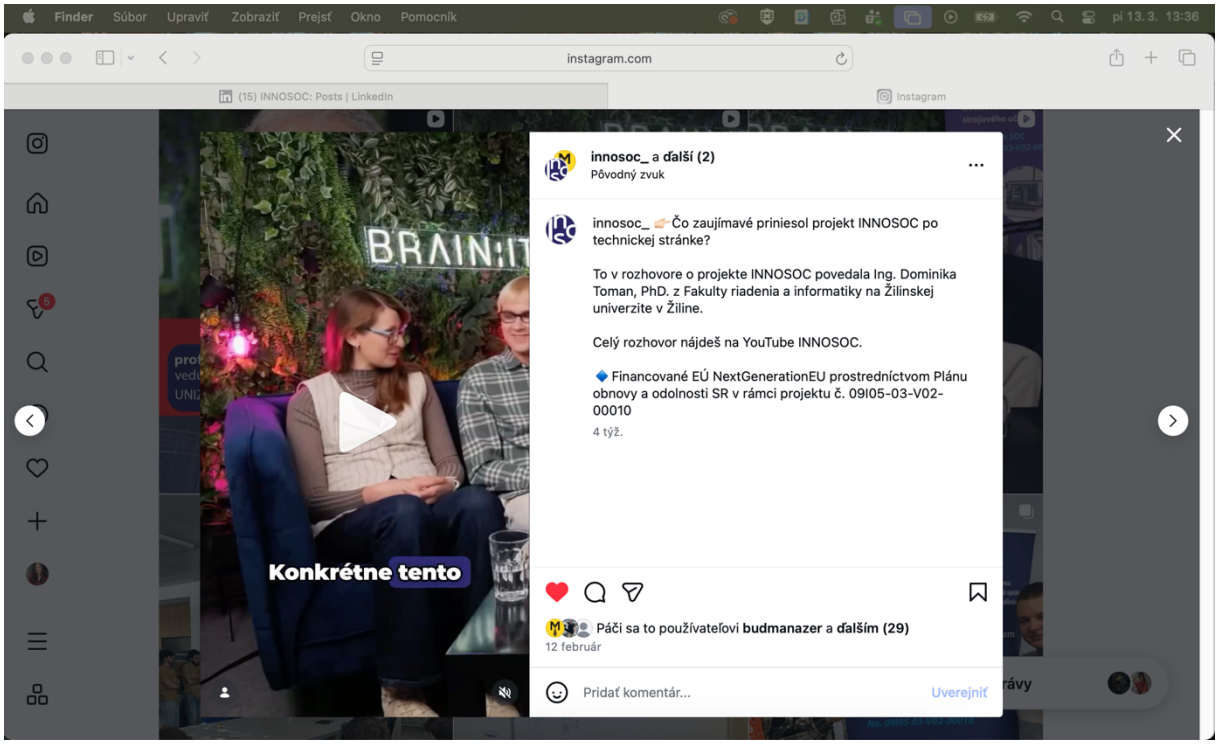
Obrázok 38: Príspevok o rozhovore s Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD. na instagramovom profile @innosoc_, Zdroj: (BRAIN:IT, 2026)

1.2.1.18 Krátke video – rozhovor s Ing. Dominikou Toman, PhD.

Dňa 12. februára 2026 bol v rámci komunikačných aktivít projektu INNOSOC na instagramovom profile @innosoc_ zverejnený príspevok odkazujúci na video-rozhovor s **Ing. Dominikou Toman, PhD.** z Fakulty riadenia a informatiky Žilinskej univerzity v Žiline. Príspevok upriamoval pozornosť na technické prínosy projektu a na vybrané inovácie, ktoré boli v rámci jeho riešenia realizované.

Obsah rozhovoru približuje technologické aspekty projektu INNOSOC, najmä vývoj a implementáciu nástrojov zameraných na podporu kybernetickej bezpečnosti a efektívnejšie monitorovanie bezpečnostných udalostí v informačných systémoch. Zároveň poukazuje na praktické prínosy projektu a jeho technologické inovácie, ktoré prispievajú k zvyšovaniu úrovne ochrany digitálnych infraštruktúr.

Príspevok zároveň informoval o dostupnosti kompletného video-rozhovoru na platforme YouTube v rámci kanála projektu INNOSOC a obsahoval informáciu o financovaní projektu z prostriedkov Európskej únie – **NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR**, v rámci projektu č. 09I05-03-V02-00010. Zverejnenie príspevku prispelo k šíreniu informácií o technologických výstupoch projektu a k zvýšeniu povedomia o jeho aktivitách.



Obrázok 39: Príspevok o rozhovore s Ing. Dominikou Toman, PhD. na instagramovom profile @innosoc_, Zdroj: (BRAIN:IT, 2026)

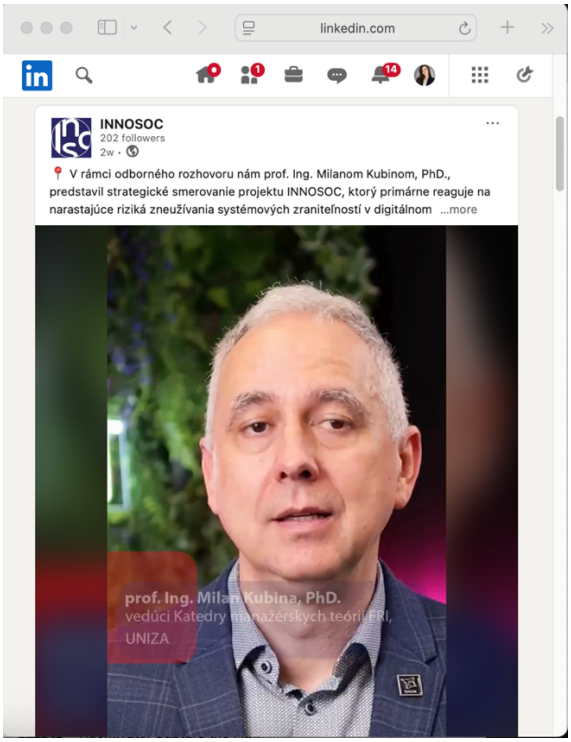
1.2.1.19 Krátke video – rozhovor s prof. Ing. Milan Kubina, PhD.

Dňa 25.februára 2026 bol v rámci komunikačných aktivít projektu INNOSOC na LinkedIn profile innosoc a instagramovom profile @innosoc_ zverejnený príspevok informujúci o odbornom rozhovore s **prof. Ing. Milanom Kubinom, PhD.** Príspevok prezentoval strategické smerovanie projektu a jeho zameranie na riešenie rastúcich rizík spojených so zneužívaním systémových zraniteľností v digitálnom prostredí.

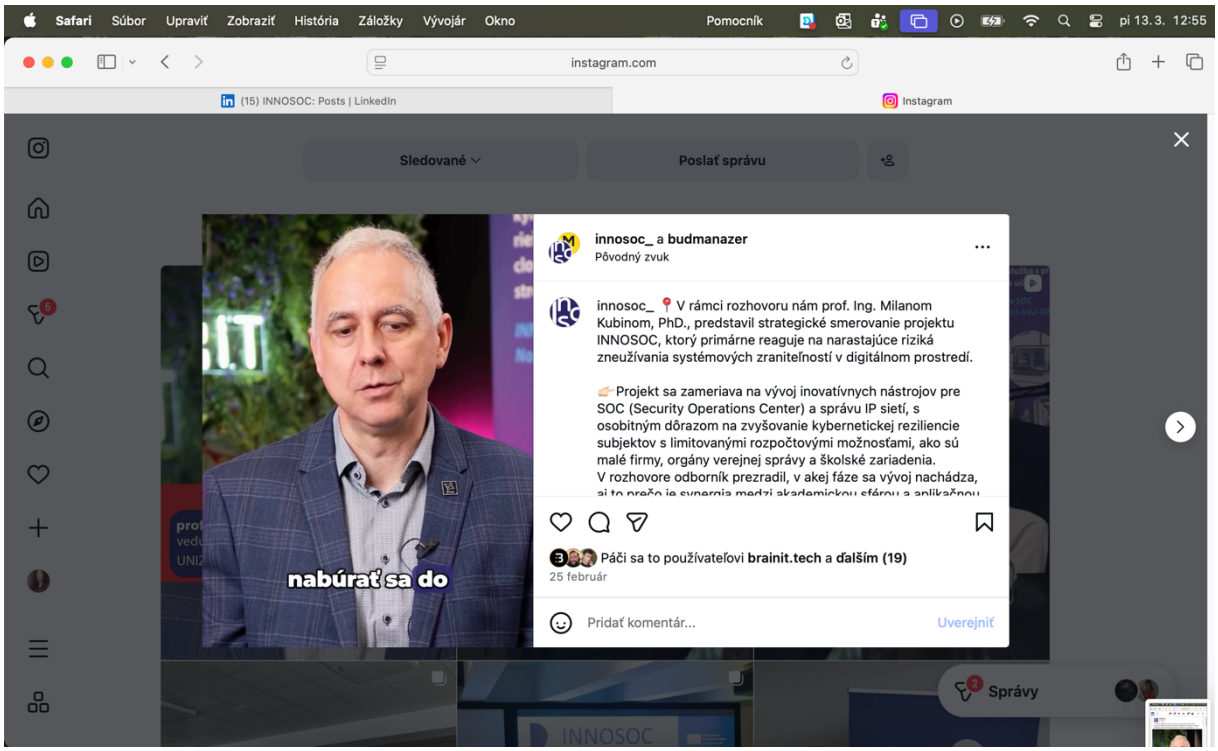
Obsah príspevku predstavil hlavné ciele projektu, najmä vývoj inovatívnych nástrojov pre Security Operations Center (SOC) a riešení pre správu IP sietí. Zdôraznený bol aj prínos projektu pre organizácie s obmedzenými finančnými zdrojmi, ako sú malé a stredné podniky, orgány verejnej správy či vzdelávacie inštitúcie, ktorým projekt pomáha zvyšovať úroveň kybernetickej bezpečnosti a reziliencie.

Príspevok zároveň poukázal na význam spolupráce medzi akademickou sférou a aplikačnou praxou, realizovanou v partnerstve so spoločnosťou BRAIN:IT, ktorá umožňuje efektívne prenášať výsledky výskumu do praktických riešení využiteľných v praxi. Súčasťou komunikácie bola aj informácia o financovaní projektu z prostriedkov Európskej únie – NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 09I05-03-V02-00010.

Zverejnenie príspevku prispelo k informovaniu odbornej aj širšej verejnosti o aktivitách projektu a podporilo šírenie povedomia o témach kybernetickej bezpečnosti.



Obrázok 40: Príspevok o rozhovore s prof. Ing. Milanom Kubinom, PhD. na LinkedIn profile @innosoc, Zdroj: (BRAIN:IT, 2026)



Obrázok 41: Príspevok o rozhovore s prof. Ing. Milanom Kubinom, PhD. na Instagramovom profile @innosoc_, Zdroj: (BRAIN:IT, 2026)

1.3 Popularizačné texty

Popularizačné texty predstavovali kľúčový nástroj pre efektívne sprostredkovanie odborných poznatkov a výsledkov projektu INNOSOC širokému spektru cieľových skupín. Ich hlavným účelom bolo transformovať komplexné technické informácie do zrozumiteľnej a pútavej formy, ktorá osloví nielen odborníkov, ale aj laickú verejnosť, študentov a potenciálnych zákazníkov.

Tieto texty slúžili ako mosty medzi vedecko-výskumnou sférou a praktickou aplikáciou, pričom zohľadňovali špecifiká jednotlivých cieľových segmentov. Pre odbornú verejnosť texty obsahovali technické detaily a metodológie, zatiaľ čo pre širokú verejnosť boli zjednodušené a doplnené o praktické príklady a vizuálne prvky.

Popularizačné články boli publikované predovšetkým prostredníctvom webovej stránky projektu, kde vytvorili ucelený informačný zdroj o kybernetickej bezpečnosti, cloudových technológiách a význame SOC riešení. Súčasne boli tieto texty adaptované pre sociálne siete v podobe kratších príspevkov, infografík a interaktívnych obsahov.

Osobitný dôraz bol kladený na edukačný charakter textov, ktoré vysvetľovali základné pojmy ako "SOC", "multitenantná architektúra", "strojové učenie v kyberbezpečnosti" či "cloudové služby" spôsobom prístupným pre rôzne úrovne technickej gramotnosti. Cieľom blo nielen informovať, ale aj vzdelávať a motivovať čitateľov k hlbšiemu záujmu o problematiku kybernetickej bezpečnosti.

Obsahová stratégia popularizačných textov vychádzala z princípu postupného budovania povedomia a dôvery. Texty boli štruktúrované do tematických celkov, ktoré pokryjú základné koncepty kybernetickej bezpečnosti, predstavia inovatívne riešenia projektu INNOSOC a ukázali ich praktické využitie v reálnych scenároch. Texty boli prípadne doplnený o vizuálne prvky ako sú infografiky alebo ilustrácie, ktoré uľahčili pochopenie zložitých technických procesov.

Dôležitým aspektom popularizačných textov bola aj ich aktuálnosť a relevantnosť k súčasným trendom v kybernetickej bezpečnosti. Tento prístup zabezpečil, že obsah zostával relevantný, atraktívny a užitočný pre čitateľov dlhodobo, pričom sa webová stránka projektu stala zdrojom informácií v oblasti kybernetickej bezpečnosti na Slovensku. Témy zvolené pre prvé popularizačné texty na stránke INNOSOC:

- Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami;
- Security Operation Center: čo to je a ako chráni vašu firmu?;
- Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany;
- Čo je cloud a na čo slúži: Základné typy a výhody cloudového úložiska;
- Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady;
- Prepojenie AI a kybernetickej bezpečnosti v praxi;
- Kybernetické útoky: Ako sa menia a prečo predstavujú čoraz väčšie riziko.

1.3.1 Realizované aktivity

Táto kapitola obsahuje opis jednotlivých popularizačných článkov, ktoré boli publikované na oficiálnej webovej stránke INNOSOC.

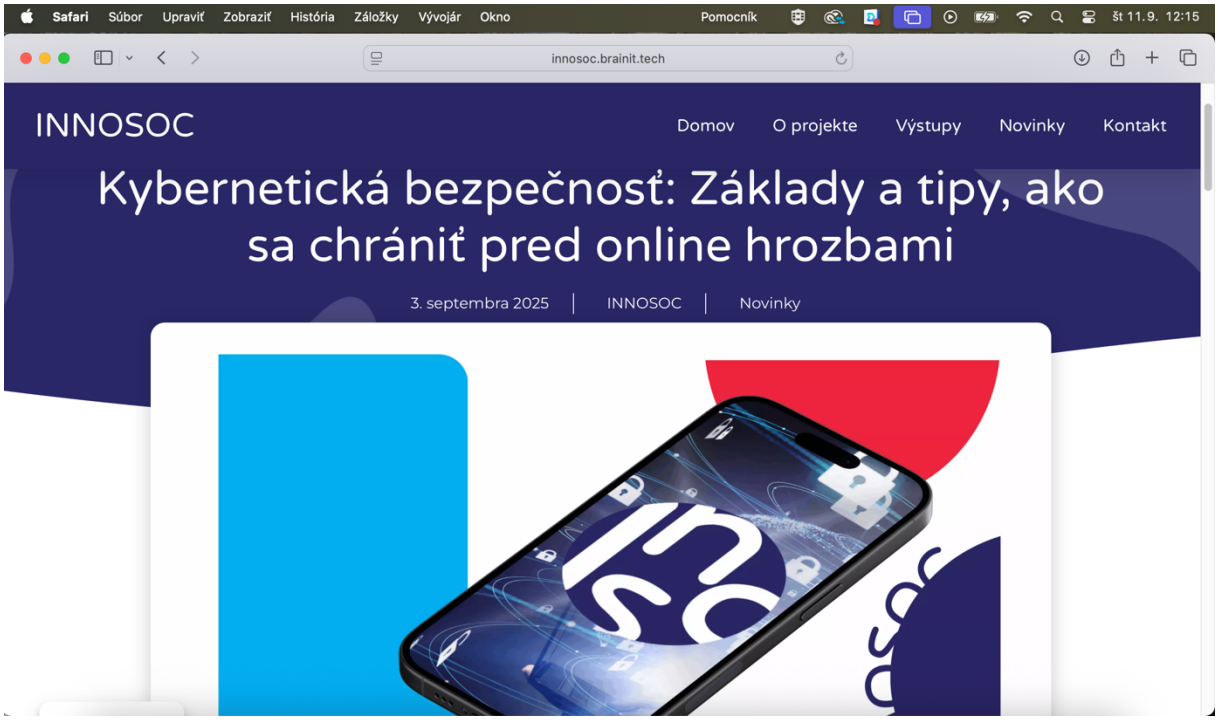
1.3.1.1 Popularizačný článok na tému Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami

Do sekcie „Novinky“ bol 3. septembra 2025 pridaný popularizačný článok na tému Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami. Cieľom článku bolo zrozumiteľnou a prístupnou formou vysvetliť základné princípy kybernetickej bezpečnosti širokej verejnosti, poukázať na aktuálne kybernetické hrozby a zdôrazniť význam prevencie v digitálnom prostredí. Obsah článku zahŕňa:

- vysvetlenie pojmu kybernetická bezpečnosť a jej významu pre jednotlivcov aj organizácie,
- opis najčastejších typov kybernetických útokov a hrozieb (napr. phishing, malvér, sociálne inžinierstvo, DDoS útoky),
- identifikáciu ohrozených typov údajov vrátane osobných, zdravotných a finančných informácií,
- rozdelenie ochrany na ľudský a technologický faktor,
- prehľad základných zásad kybernetickej bezpečnosti, ako sú silné heslá, dvojfaktorová autentifikácia, pravidelné aktualizácie, zálohovanie dát a používanie antivírusu a firewallu,
- dôraz na prevenciu ako kľúčový prvok ochrany pred kybernetickými rizikami.

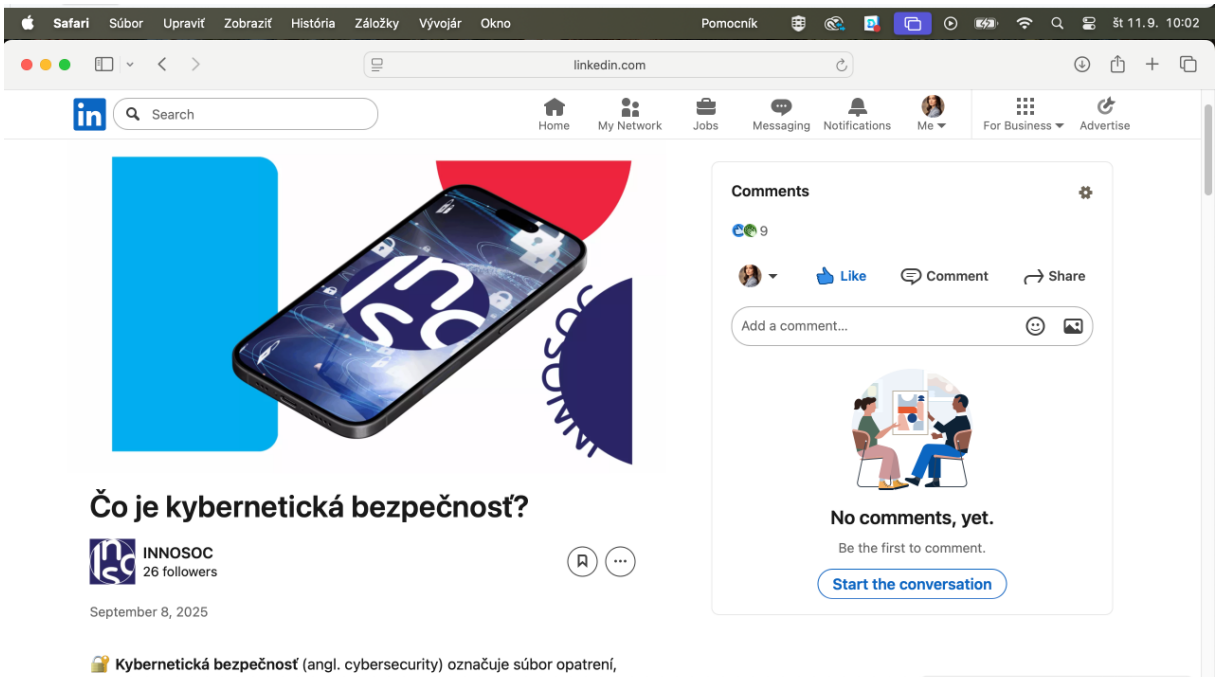
Článok slúži ako edukačný a osvetový výstup projektu, ktorého cieľom je zvýšiť povedomie o kybernetickej bezpečnosti, podporiť zodpovedné správanie používateľov v online priestore a prispieť k znižovaniu rizík spojených s digitálnymi hrozbami.

Celé znenie článku sa nachádza v prílohe 10 – Článok: Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami.



Obrázok 42 Popularizačný článok na tému kybernetická bezpečnosť, Zdroj: (BRAIN:IT, 2025)

Pre väčšie zasiahnutie publika bol rovnaký popularizačný text zverejnený na LinkedIn stránke @INNOSOC s cieľom zasiahnuť odborníkov a študentov vysokých škôl. Tento článok bol zverejnený 8.9.2025.



Obrázok 43 Popularizačný článok na tému kybernetická bezpečnosť na LinkedIn stránke @INNOSOC, Zdroj: (BRAIN:IT, 2025)

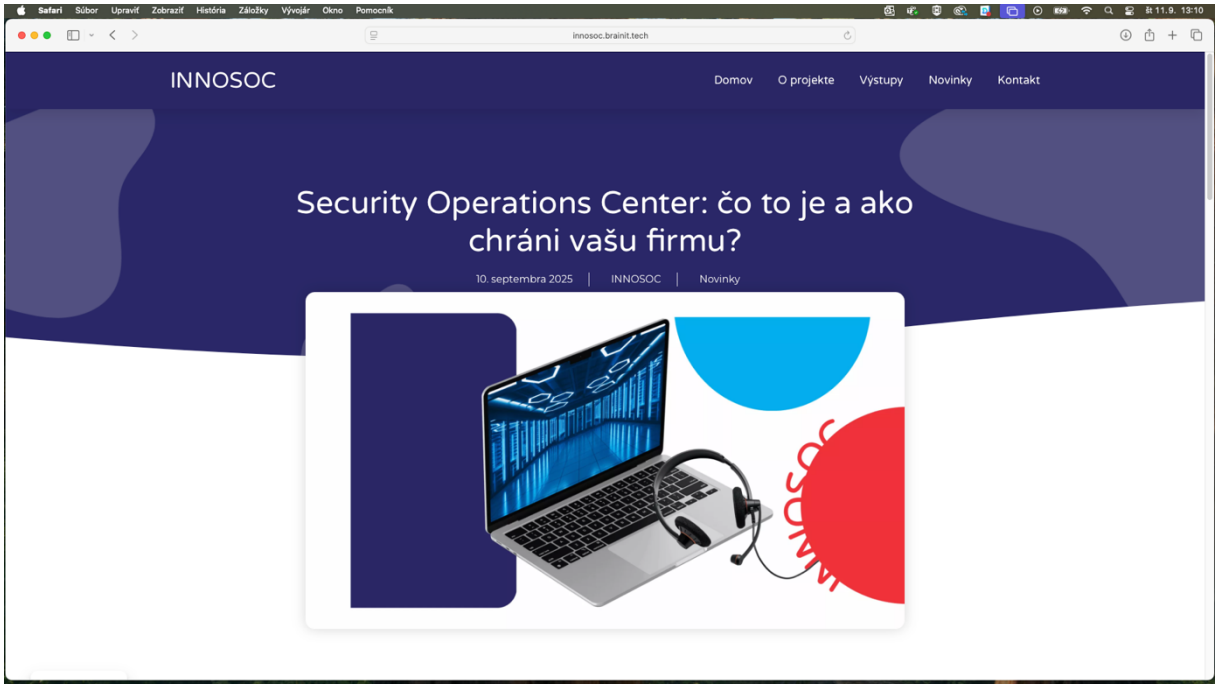
1.3.1.2 Popularizačný článok na tému Security Operations Center: čo to je a ako chráni vašu firmu?

Dňa 10. septembra 2025 bol v sekcii „Novinky“ zverejnený edukačný článok na tému „Security Operations Center: čo to je a ako chráni vašu firmu?“. Cieľom článku bolo priblížiť pojem Security Operations Center ako kľúčový prvok moderného prístupu ku kybernetickej bezpečnosti a vysvetliť jeho význam pri ochrane digitálnych aktív organizácií v prostredí rastúcich kybernetických hrozieb. Obsah článku sa zameriava najmä na:

- vysvetlenie úlohy SOC ako centralizovaného a nepretržitého bezpečnostného strediska,
- definovanie hlavného poslania SOC, ktorým je minimalizácia dopadov kybernetických incidentov a proaktívna ochrana organizácie,
- opis spôsobu fungovania SOC vrátane práce bezpečnostných analytikov a využívania pokročilých bezpečnostných technológií,
- predstavenie základných modelov SOC (interný, externý a hybridný),
- prehľad hlavných funkcií Security Operations Center, ako sú monitorovanie a detekcia incidentov, riadenie bezpečnostných incidentov a riadenie problémov,
- zdôraznenie významu procesov, dokumentácie a interných bezpečnostných politík ako súčasti efektívneho fungovania SOC.

Článok slúži ako odborný a osvetový výstup projektu, ktorého cieľom je zvýšiť informovanosť o praktickom fungovaní Security Operations Center, podporiť systematický prístup ku kybernetickej bezpečnosti v organizáciách a poukázať na dôležitosť prevencie, monitoringu a riadenia bezpečnostných incidentov v digitálnom prostredí.

Celé znenie článku sa nachádza v prílohe 11 – Článok: Security Operations Center: čo to je a ako chráni vašu firmu?



Obrázok 44 Popularizačný článok na tému Security Operations Center, Zdroj: (BRAIN:IT, 2025)

1.3.1.3 Popularizačný článok na tému Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany

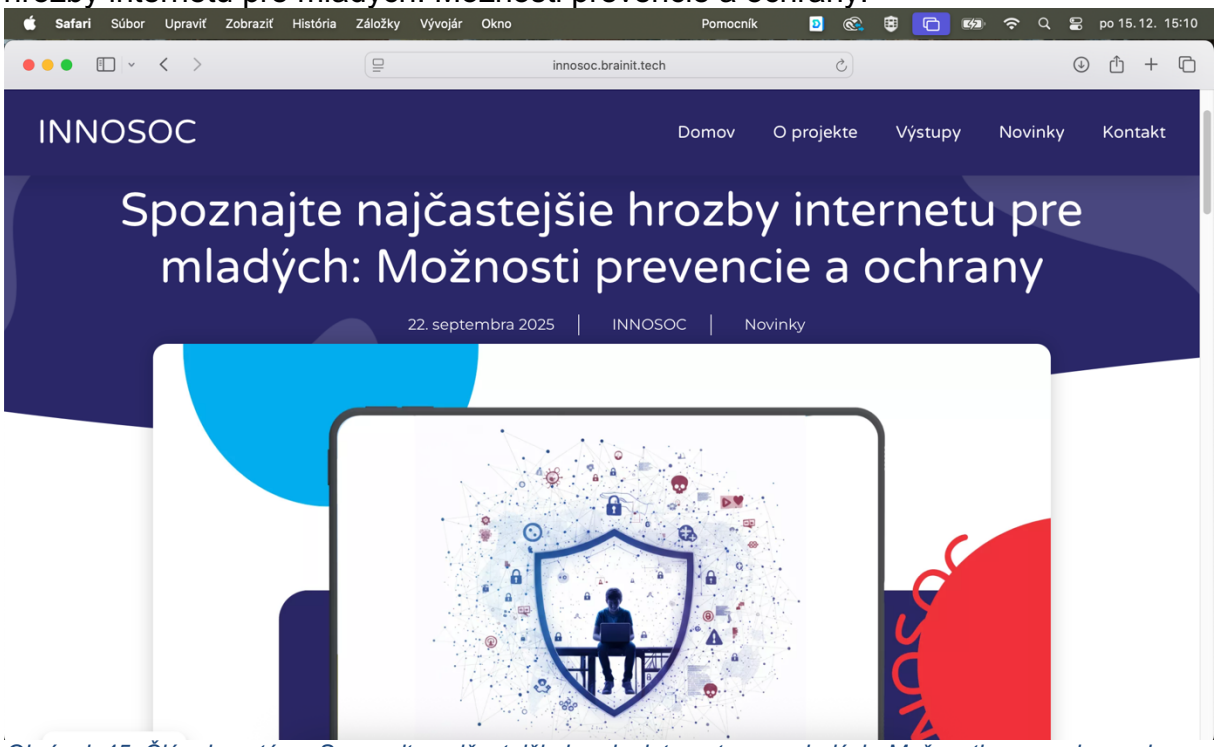
V rámci projektu bol dňa 22. septembra publikovaný edukačno-osvetový článok zameraný na riziká digitálneho a online prostredia pre mladú generáciu, ktorý bol zverejnený na webovej stránke v sekcii „Novinky“. Cieľom článku bolo zvýšiť povedomie o bezpečnosti mladých v online priestore, poukázať na najčastejšie digitálne hrozby, ktorým sú mladí ľudia vystavení, a poskytnúť praktické odporúčania pre prevenciu a ochranu v každodennom digitálnom živote. Obsah článku sa zameriava najmä na:

- charakteristiku súčasnej generácie vyrastajúcej v informačnom a technologickom veku,
- identifikáciu hlavných hrozieb digitálneho sveta pre mladých, ako sú nevhodný a nebezpečný obsah, komunikácia na sociálnych sieťach, zdieľanie intímneho obsahu, internetové podvody, online šikana, diskriminácia a nenávistné prejavy,
- riziká spojené so závislosťou od technológií, sociálnych sietí a digitálnych vzťahov, vrátane psychických dopadov (napr. FOMO, FOBO, sociálna izolácia),
- význam prevencie a vzdelávania v oblasti digitálnej bezpečnosti ako základného nástroja ochrany mladých,
- bezpečnostné odporúčania pre zodpovedné správanie v online priestore, najmä pri zdieľaní osobných údajov, fotografií a pri komunikácii s neznámymi osobami,
- zdôraznenie úlohy rodiny a domáceho prostredia ako kľúčového prvku prevencie digitálnych rizík.

Článok predstavuje edukačný a preventívny výstup projektu, ktorého cieľom je podporiť bezpečné a zodpovedné správanie mladých ľudí v digitálnom prostredí,

posilniť informovanosť rodičov a pedagógov a prispieť k budovaniu zdravých hraníc a bezpečného online správania v súčasnej spoločnosti.

Celé znenie článku sa nachádza v prílohe 12 – Článok: Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany.



Obrázok 45: Článok na tému Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany, Zdroj: (BRAIN:IT, 2025)

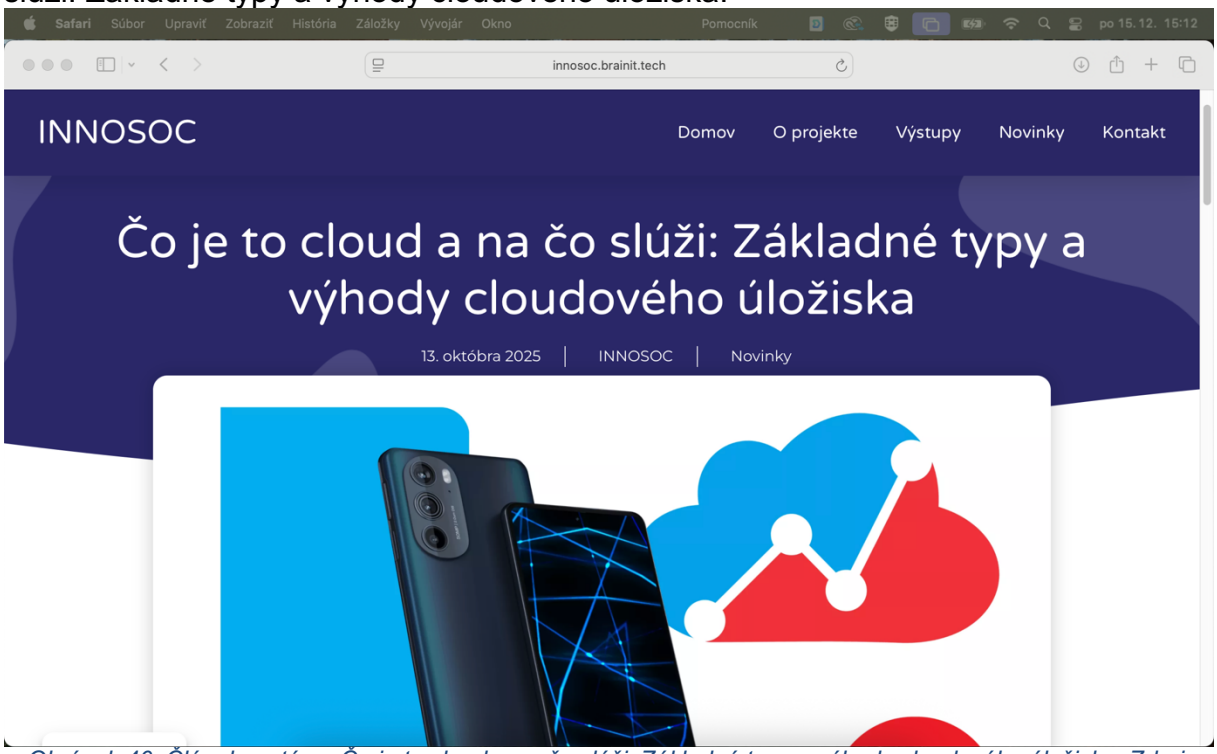
1.3.1.4 Popularizačný článok na tému Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska

V rámci projektu bol vytvorený a publikovaný odborný edukačný článok zameraný na cloudové služby a moderné spôsoby ukladania a správy dát, ktorý bol zverejnený na webovej stránke vytvorenej v rámci projektu. Cieľom článku bolo zrozumiteľnou formou vysvetliť pojem cloud, jeho praktické využitie v každodennom aj firemnom prostredí a poukázať na základné výhody a riziká spojené s využívaním cloudových riešení. Obsah článku sa zameriava najmä na:

- vysvetlenie pojmu cloud a princípov fungovania cloudových služieb,
- prehľad foriem využitia cloudu, ako je web hosting, zdieľanie súborov, distribúcia softvéru a cloud computing,
- predstavenie základných typov cloudových riešení (verejný, súkromný a hybridný cloud) vrátane ich charakteristík,
- porovnanie výhod a nevýhod cloudových služieb z hľadiska produktivity, efektivity, nákladov a bezpečnosti,
- upozornenie na bezpečnostné riziká a význam ochrany citlivých osobných a firemných údajov pri ukladaní dát do cloudu.

Článok predstavuje odborný a osvetový výstup projektu, ktorého cieľom je zvýšiť digitálnu gramotnosť používateľov, podporiť informované rozhodovanie pri výbere cloudových riešení a prispieť k lepšiemu porozumeniu moderných technológií ukladania a správy dát v digitálnom prostredí.

Celé znenie článku sa nachádza v prílohe 13 – Článok: Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska.



Obrázok 46: Článok na tému Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska, Zdroj: (BRAIN:IT, 2025)

1.3.1.5 Popularizačný článok na tému Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady

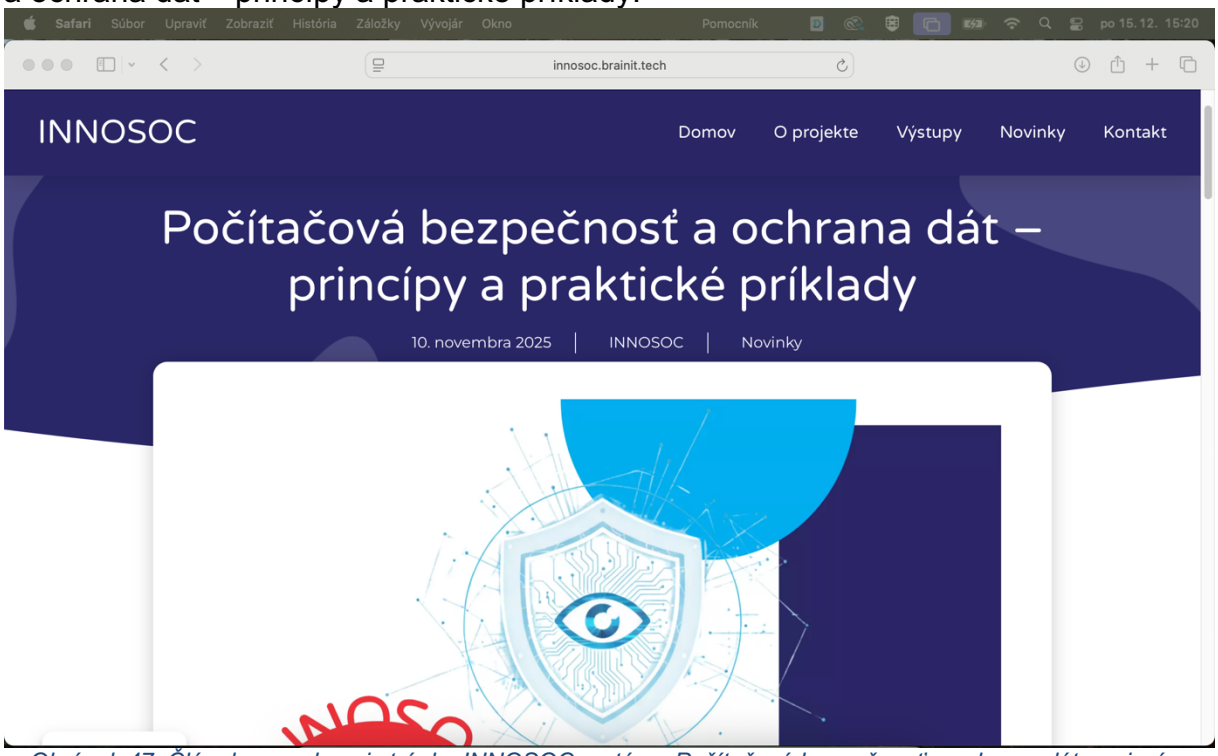
Dňa 10. novembra 2025 bol vytvorený a publikovaný odborný edukačný článok zameraný na počítačovú bezpečnosť a ochranu dát, ktorý bol zverejnený na webovej stránke vytvorenej v rámci projektu. Cieľom článku bolo vysvetliť základné princípy ochrany dát a informácií v online prostredí a priblížiť koncept bezpečnostnej triády (CIA – dôvernosť, integrita, dostupnosť) ako kľúčový základ každej bezpečnostnej stratégie v organizáciách aj v bežnom digitálnom živote. Obsah článku sa zameriava najmä na:

- vysvetlenie významu počítačovej a kybernetickej bezpečnosti pri práci s digitálnymi údajmi,
- definovanie troch základných princípov bezpečnostnej triády – dôvernosti, integrity a dostupnosti,
- prepojenie princípov ochrany dát s platnou slovenskou a európskou legislatívou v oblasti ochrany osobných údajov,
- praktickú aplikáciu jednotlivých princípov v každodennej praxi prostredníctvom konkrétnych bezpečnostných opatrení,
- príklady technických a organizačných nástrojov na ochranu dát, ako sú šifrovanie, riadenie prístupov, viacfaktorová autentifikácia, elektronický podpis, zálohovanie a monitoring dostupnosti,
- zdôraznenie potreby rovnováhy medzi jednotlivými prvkami bezpečnostnej triády pri návrhu bezpečnostných politík.

Článok predstavuje odborný a edukačný výstup projektu, ktorého cieľom je zvýšiť povedomie o ochrane dát a informácií, podporiť zodpovedné správanie

používateľov v digitálnom prostredí a poskytnúť praktický základ pre budovanie efektívnych bezpečnostných opatrení v organizáciách aj u jednotlivcov.

Celé znenie článku sa nachádza v prílohe 14 – Článok: Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady.



Obrázok 47: Článok na webovej stránke INNOSOC na tému Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady, Zdroj: (BRAIN:IT, 2025)

1.3.1.6 Popularizačný článok na tému Prepojenie AI a kybernetickej bezpečnosti v praxi

V sekcii „Novinky“ na webovej stránke projektu INNOSOC bol dňa 16. decembra 2025 zverejnený popularizačný článok zameraný na tému využitia umelej inteligencie v oblasti kybernetickej bezpečnosti. Článok približuje aktuálne trendy v oblasti kybernetických hrozieb a poukazuje na rastúci význam moderných technologických nástrojov pri ochrane informačných systémov.

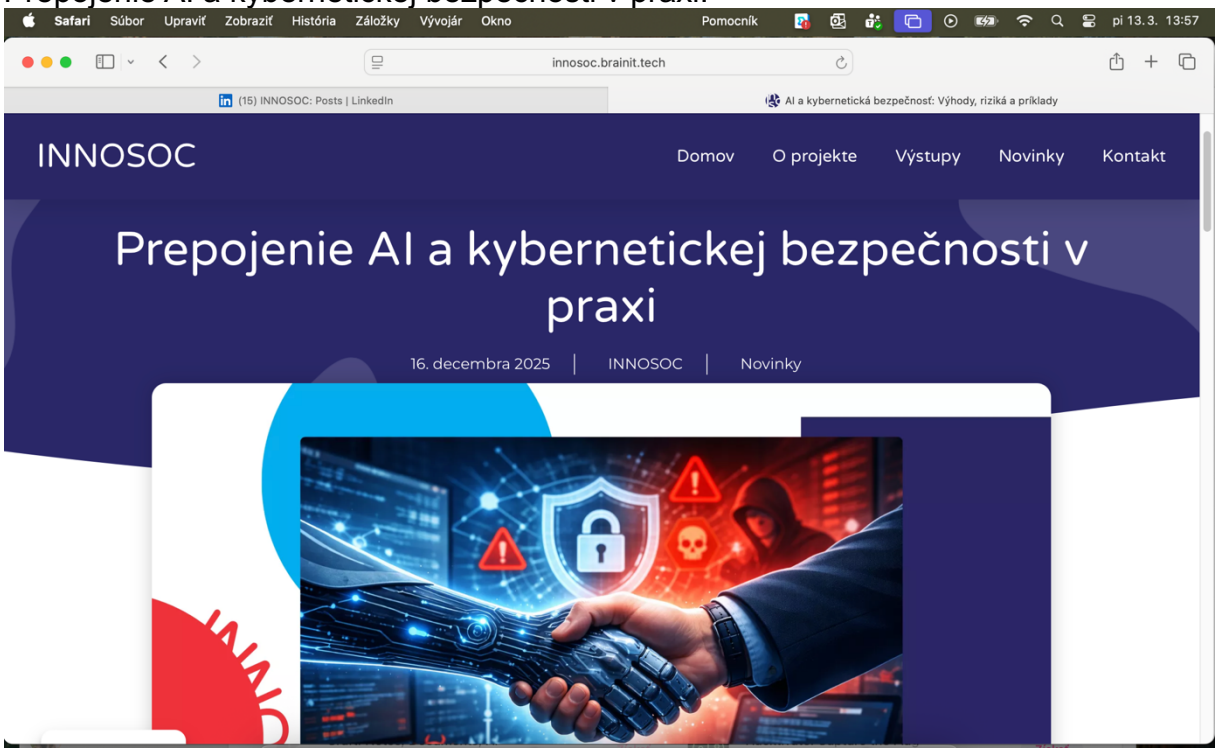
Obsah článku vysvetľuje možnosti využitia umelej inteligencie pri detekcii, prevencii a riešení kybernetických incidentov. Zdôraznené sú najmä schopnosti AI analyzovať veľké objemy dát v reálnom čase, identifikovať anomálie v správaní používateľov a systémov, predpovedať potenciálne útoky a automatizovať reakcie na bezpečnostné incidenty. Zároveň článok upozorňuje aj na limity umelej inteligencie a poukazuje na skutočnosť, že AI by nemala fungovať ako samostatné riešenie, ale ako nástroj podporujúci prácu bezpečnostných analytikov.

Súčasťou článku je aj analýza rizík spojených so zneužívaním umelej inteligencie zo strany útočníkov, napríklad pri automatizovaných útokoch, generovaní phishingových kampaní, tvorbe škodlivého kódu alebo využívaní technológií deepfake na sociálne inžinierstvo. Článok preto zdôrazňuje potrebu vyváženého prístupu, ktorý kombinuje technologické nástroje umelej inteligencie s odborným ľudským dohľadom.

Publikovanie článku na webovej stránke projektu prispieva k popularizácii tém kybernetickej bezpečnosti, k šíreniu poznatkov o možnostiach využitia umelej inteligencie v tejto oblasti a k zvyšovaniu povedomia odbornej aj širšej verejnosti o

aktuálnych bezpečnostných výzvach. Článok je výstupom projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia“ (kód projektu 09I05-03-V02-00010), financovaného z prostriedkov Európskej únie – NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR.

Celé znenie článku sa nachádza v prílohe 21 – Popularizačný článok na tému Prepojenie AI a kybernetickej bezpečnosti v praxi.



Obrázok 48:Popularizačný článok na tému Prepojenie AI a kybernetickej bezpečnosti v praxi, Zdroj: (BRAIN:IT, 2025)

1.3.1.7 Popularizačný článok na tému Kybernetické útoky: Ako sa menia a prečo predstavujú čoraz väčšie riziko

V sekcii „Novinky“ na webovej stránke projektu INNOSOC bol dňa 19. decembra 2025 zverejnený popularizačný článok zameraný na problematiku narastajúcej sofistikovanosti kybernetických útokov a ich dopadov na jednotlivcov, firmy aj verejné inštitúcie. Článok vysvetľuje, že súčasné kybernetické hrozby už nie sú dielom izolovaných jednotlivcov, ale často ich realizujú organizované skupiny využívajúce pokročilé technológie, automatizačné nástroje a prvky umelej inteligencie.

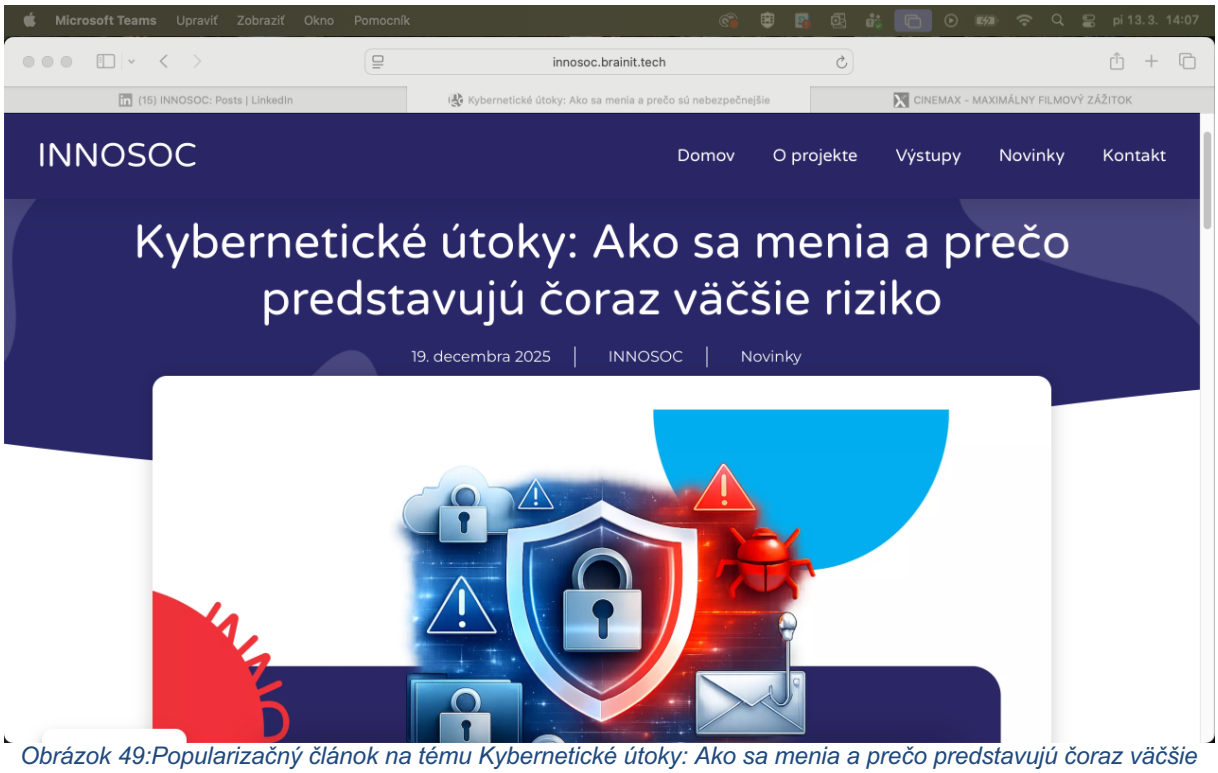
Obsah článku približuje hlavné faktory, ktoré prispievajú k zvyšovaniu komplexnosti kybernetických útokov, ako sú organizovaná spolupráca útočníkov, využívanie pokročilých techník vrátane sociálneho inžinierstva, rastúca digitalizácia spoločnosti a rozšírené využívanie umelej inteligencie pri príprave a realizácii útokov. Článok zároveň poukazuje na praktické dôsledky kybernetických incidentov, najmä zneužitie citlivých údajov, finančné straty, narušenie dôvery či zvýšené náklady na zabezpečenie informačných systémov.

Súčasťou článku je aj vysvetlenie významu systematického prístupu k ochrane údajov a kybernetickej bezpečnosti. Zdôrazňuje sa potreba kombinácie technických

bezpečnostných riešení, nepretržitého monitorovania systémov a zodpovedného prístupu používateľov k správe a ochrane dát.

Publikovanie článku na webovej stránke projektu prispieva k popularizácii tém kybernetickej bezpečnosti, k šíreniu informácií o aktuálnych bezpečnostných hrozbách a k zvyšovaniu povedomia verejnosti o potrebe systematickej ochrany digitálnych údajov. Článok je výstupom projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia“ (kód projektu 09I05-03-V02-00010), financovaného z prostriedkov Európskej únie – NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR.

Celé znenie článku sa nachádza v prílohe 22 – Popularizačný článok na tému Prepojenie AI a kybernetickej bezpečnosti v praxi.



Obrázok 49:Popularizačný článok na tému Kybernetické útoky: Ako sa menia a prečo predstavujú čoraz väčšie riziko, Zdroj: (BRAIN:IT, 2025)

1.3.1.8 Popularizačný článok na tému Automatizácia a hlboké strojové učenie v kybernetickej bezpečnosti

V sekcii „Novinky“ na webovej stránke projektu INNOSOC bol dňa 21. januára 2026 zverejnený popularizačný článok zameraný na využitie automatizácie a technológií strojového učenia v oblasti kybernetickej bezpečnosti. Článok vysvetľuje, prečo je automatizácia reakcií na bezpečnostné incidenty nevyhnutná v prostredí, kde objem bezpečnostných udalostí a dát neustále rastie a ich manuálne spracovanie je čoraz náročnejšie.

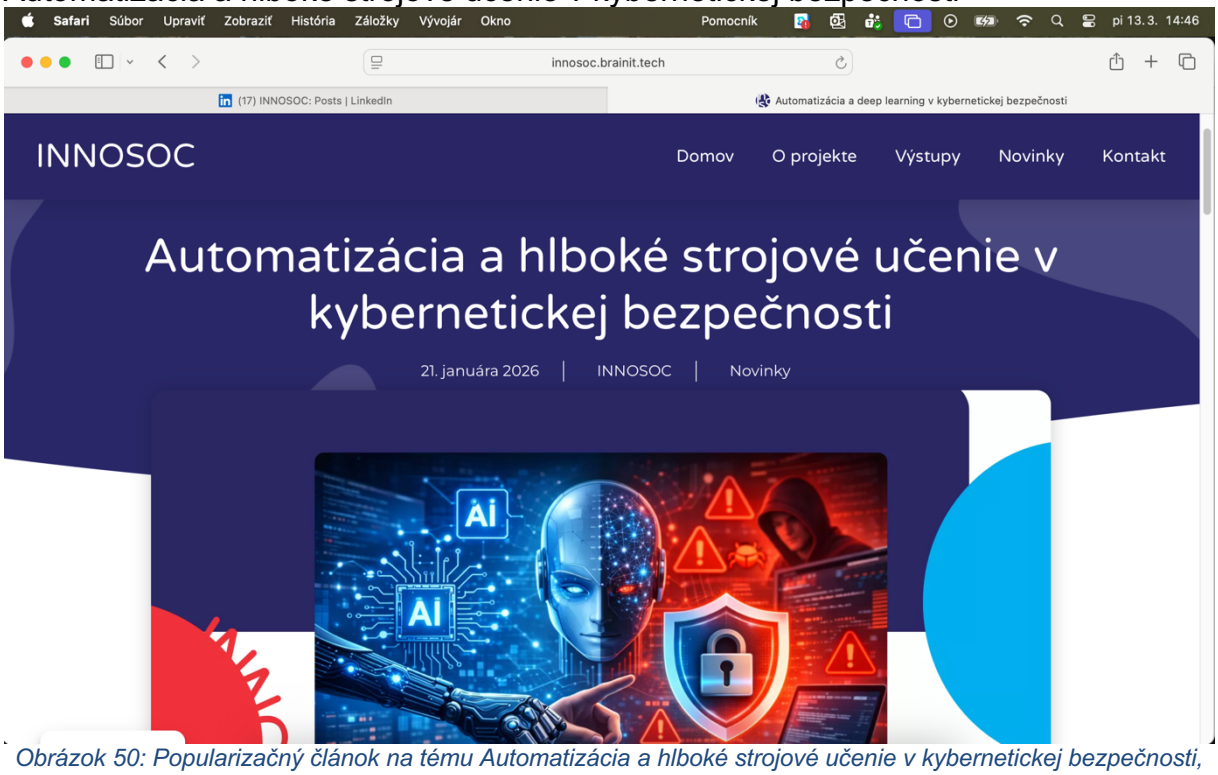
Obsah článku približuje princípy fungovania strojového učenia a hlbokého strojového učenia (deep learning) pri detekcii kybernetických hrozieb. Vysvetľuje, ako tieto technológie dokážu analyzovať veľké množstvo bezpečnostných dát, identifikovať anomálie v správaní systémov, používateľov a zariadení a prispieť k včasnému odhaleniu kybernetických útokov. Súčasťou článku je aj vysvetlenie praktického

využitia automatizovaných bezpečnostných nástrojov, napríklad pri analýze správania v sieti, predikcii bezpečnostných incidentov alebo pri automatizovanej reakcii na hrozby prostredníctvom riešení typu SOAR.

Článok zároveň upozorňuje aj na limity automatizácie a využívania umelej inteligencie v kybernetickej bezpečnosti, najmä na riziko falošných poplachov alebo závislosť modelov od kvality tréningových dát. Zdôrazňuje sa preto potreba spolupráce technologických nástrojov s ľudským faktorom, pričom bezpečnostní analytici zohrávajú kľúčovú úlohu pri interpretácii výsledkov, vyšetrovaní incidentov a nastavovaní bezpečnostných stratégií.

Publikovanie článku na webovej stránke projektu prispieva k popularizácii tém kybernetickej bezpečnosti a k šíreniu poznatkov o moderných technologických prístupoch k ochrane informačných systémov. Článok je výstupom projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia“ (kód projektu 09I05-03-V02-00010), financovaného z prostriedkov Európskej únie – NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR.

Celé znenie článku sa nachádza v prílohe 23 – Popularizačný článok na tému Automatizácia a hlboké strojové učenie v kybernetickej bezpečnosti



Obrázok 50: Popularizačný článok na tému Automatizácia a hlboké strojové učenie v kybernetickej bezpečnosti, Zdroj: (BRAIN:IT, 2026)

1.4 Audiovizuálny obsah

Videá a iný audiovizuálny obsah sú vhodnou formou pre lepšie zaujatie pozornosti najmä pri komunikovaní jednoduchších myšlienok pre širokú verejnosť, študentov vysokej školy a študentov strednej školy.

Ich hlavnou úlohou bolo dynamicky a pútavo predstaviť komplexné technické procesy a výhody SOC riešenia prostredníctvom kombinovaného audiovizuálneho

obsahu, ktorý mal osloviť širokú škálu cieľových skupín. Boli zdieľané najmä na sociálnych sieťach a webovej stránke projektu.

Videá boli prispôsobené špecifikám jednotlivých platforiem a cieľových segmentov, pričom pre sociálne siete boli vytvorené kratšie formáty s výraznou vizuálnou stránkou, zatiaľ čo pre webovú stránku a odborné prezentácie boli pripravené detailnejšie a technicky orientované videá. Obsah zahŕňal vysvetlenia fungovaní SOC systémov, rozhovory s odborníkmi a vyjadrenia od partnerov projektu.

Promo videá slúžili ako kľúčový nástroj pre vzdelávanie študentov a zvyšovanie digitálnej gramotnosti širokej verejnosti, pričom vysvetľovali základné pojmy kybernetickej bezpečnosti.

Produkcia videí zahŕňala využitie moderných a profesionálnych produkčných nástrojov vizualizácie a postprodukcie, ktoré umožnili efektívne prezentovať abstraktné koncepty kybernetickej bezpečnosti. Videá obsahovali profesionálne nahovorené komentáre, kvalitné grafické prvky a hudbu, ktorá podčiarkne inovatívny charakter projektu.

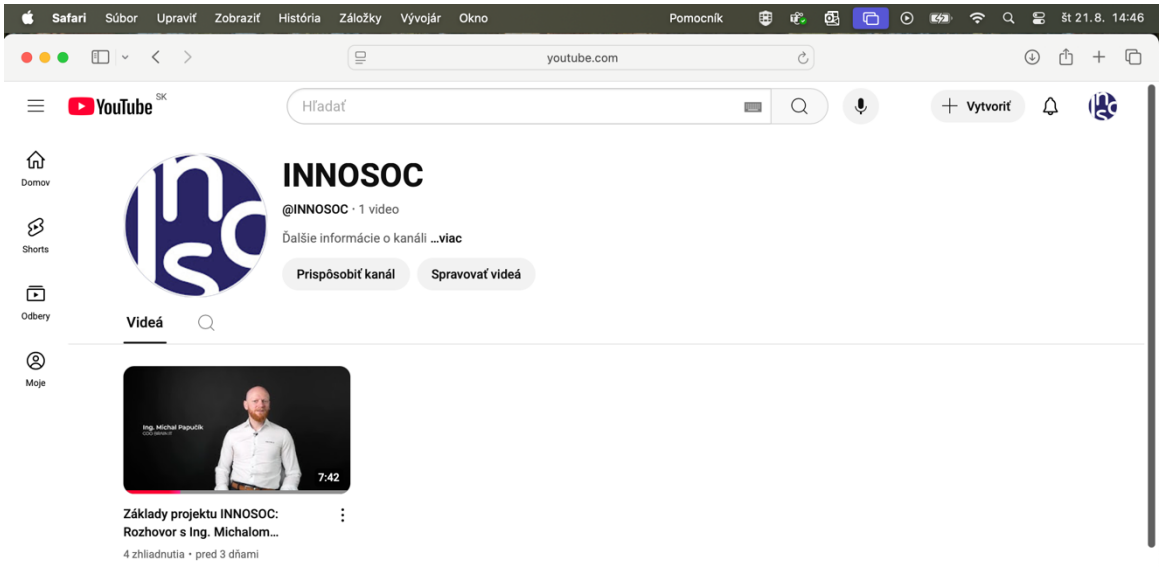
Súčasne boli videá dostupné s titulkami v slovenskom alebo anglickom jazyku, čo rozšíri ich dosah na medzinárodnú úroveň a zvýši ich využiteľnosť pre rôzne cieľové skupiny.

1.4.1 Realizované aktivity

Táto kapitola obsahuje opis jednotlivých audiovizuálnych výstupov, ktoré boli publikované na oficiálnej webovej stránke INNOSOC, Youtube kanály INNOSOC a na sociálnych sieťach.

1.4.1.1 Vytvorenie účtu na platforme YouTube

Pre publikáciu videí – najmä odborných rozhovorov či rôznych aktivít vo forme podujatí bol vytvorený kanál na platforme YouTube s názvom @INNOSOC. Ten bude slúžiť ako podporný nástroj a bude využitý pre zdieľanie spomínaných videí v iných kanáloch, ako je napríklad webová stránka. Kanál bol vytvorený aj z dôvodu možnosti archivácie všetkého video obsahu a jeho ľahkej dostupnosti pre odbornú aj laickú verejnosť.

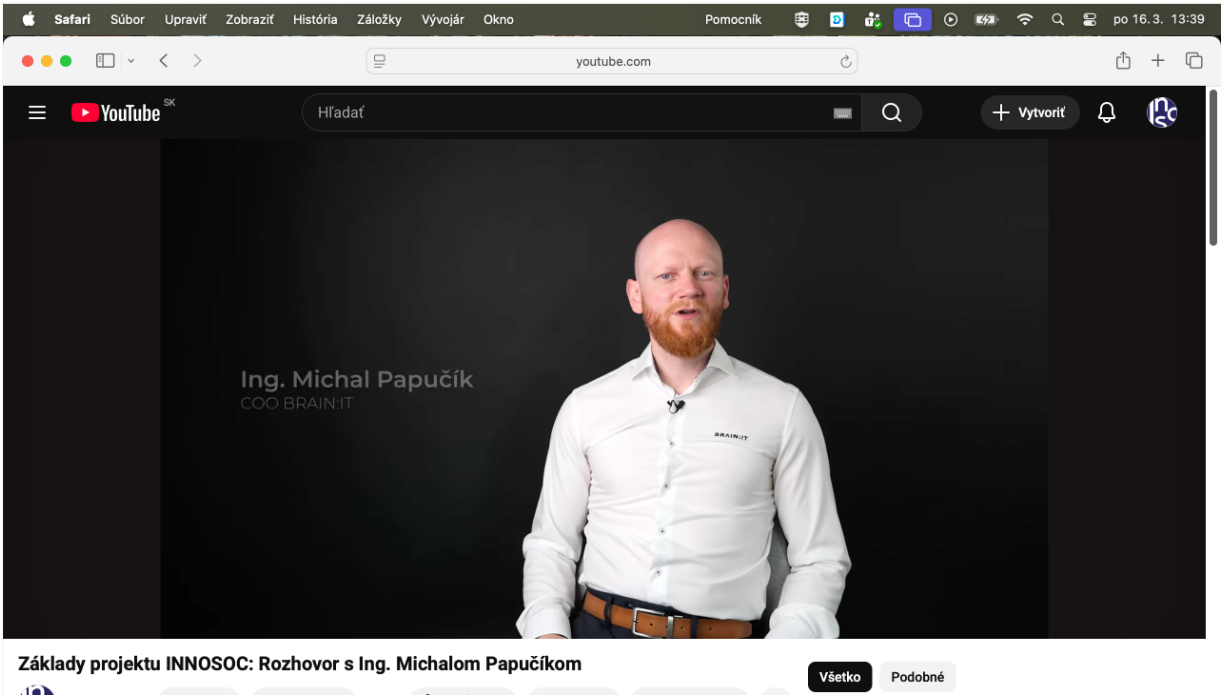


Obrázok 51: YouTube kanál @INNOSOC, Zdroj: (BRAIN:IT, 2025)

1.4.1.2 Videorozhovor s Ing. Michal Papučík

Cieľom videorozhovoru s Ing. Michalom Papučíkom, COO spoločnosti BRAIN:IT, ktorý na projekte participuje ako výskumník, analytik a architekt informačných systémov, bolo priniesť širokej verejnosti základné informácie o projekte. Videorozhovor informuje o cieli, potrebe vzniku, výzvach, na ktoré projekt reaguje, prínosoch, využitých technológiách, prepojení akademickej obce s biznis sférou, metódach a medzinárodných postupoch, ktoré sa v projekte využívajú, a zároveň ponúka osobný pohľad na projekt a skúsenosť Ing. Michala Papučíka.

Celý prepis rozhovoru s Ing. Michalom Papučíkom sa nachádza v prílohe 15-Rozhovor s Ing. Michalom Papučíkom.



Obrázok 52: Videorozhovor s Ing. Michal Papučík, Zdroj: (BRAIN:IT, 2025)

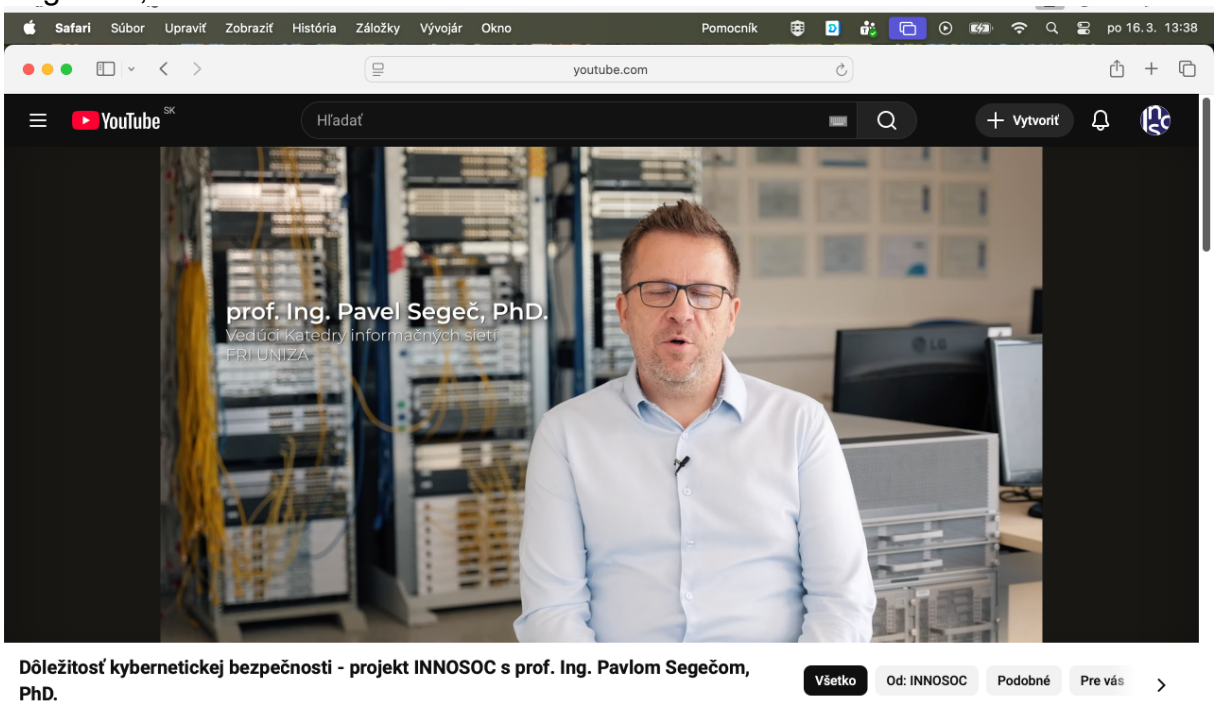
1.4.1.3 Videorozhovor s prof. Ing. Pavel Segeč, PhD.

Cieľom rozhovoru bolo priblížiť význam kybernetickej bezpečnosti v súčasnom digitálnom prostredí, poukázať na rastúce kybernetické hrozby a vysvetliť úlohu projektu INNOSOC pri budovaní systematickej a centralizovanej ochrany organizácií a vzdelávacích inštitúcií. Obsah rozhovoru sa zameriava najmä na:

- význam kybernetickej bezpečnosti pre organizácie všetkých veľkostí v kontexte rastúcej digitalizácie,
- úlohu Fakulty riadenia a informatiky UNIZA ako hlavného partnera projektu a poskytovateľa vedecko-výskumných a vývojových kapacít,
- identifikáciu najčastejších kybernetických hrozieb, ako sú phishing, ransomvér a pokročilé pretrvávajúce hrozby (APT),
- vysvetlenie konceptu Security Operations Center (SOC) ako centrálneho prvku ochrany, postaveného na pilieroch ľudí, procesov a technológií,
- dopady novej smernice NIS2 na požiadavky v oblasti riadenia a reportovania kybernetických incidentov,
- praktické fungovanie SOC systémov založených na zbere, korelácii a analýze veľkého objemu bezpečnostných dát v reálnom čase.

Rozhovor predstavuje odborný, prezentačný a osvetový výstup projektu, ktorý prepája vedecko-výskumný pohľad s praktickými dopadmi na bezpečnosť organizácií. Zároveň slúži ako nástroj na zvyšovanie povedomia o význame kybernetickej bezpečnosti a o prínosoch projektu INNOSOC pre akademickú aj aplikačnú prax.

Celý prepis rozhovoru sa nachádza v prílohe 16 – Rozhovor s prof. Ing. Pavlom Segečom, PhD.



Obrázok 53: Videorozhovor s prof. Ing. Pavel Segeč, PhD., Zdroj: (BRAIN:IT, 2025)

1.4.1.4 Videorozhovor s Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD.

Dňa 22.januára 2026 bolo na YouTube kanál INNOSOC pridané video s názvom „O projekte INNOSOC s Dominikou Toman a Martinom Mičiakom“. Video formou rozhovoru približuje detaily výskumného projektu, jeho ciele, praktické prínosy a výzvy spojené s jeho riadením. V diskusii boli rozoberané nasledujúce kľúčové témy:

- Zameranie a cieľ projektu: Projekt INNOSOC prepája výskum, prax a inovácie v oblasti kybernetickej bezpečnosti a Security Operation Centers (SOC). Jeho hlavným cieľom je navrhnúť technologické riešenie pre organizácie (najmä verejnú správu a podniky), ktoré si nemôžu dovoliť drahé komerčné riešenia. Toto riešenie je postavené na integrácii vhodných open-source komponentov.
- Spolupráca a obsadenie: Projekt predstavuje unikátne prepojenie akademického prostredia (Fakulta riadenia a informatiky Žilinskej univerzity v Žiline) a biznis partnera (spoločnosť BRAIN:IT). Hostia Dominika Toman a Martin Mičiak z Katedry manažérskych teórií vysvetlili, že ich úlohou v projekte je predovšetkým koordinácia, riadenie a projektový manažment, zatiaľ čo technickú stránku zastrešuje Katedra informačných sietí.

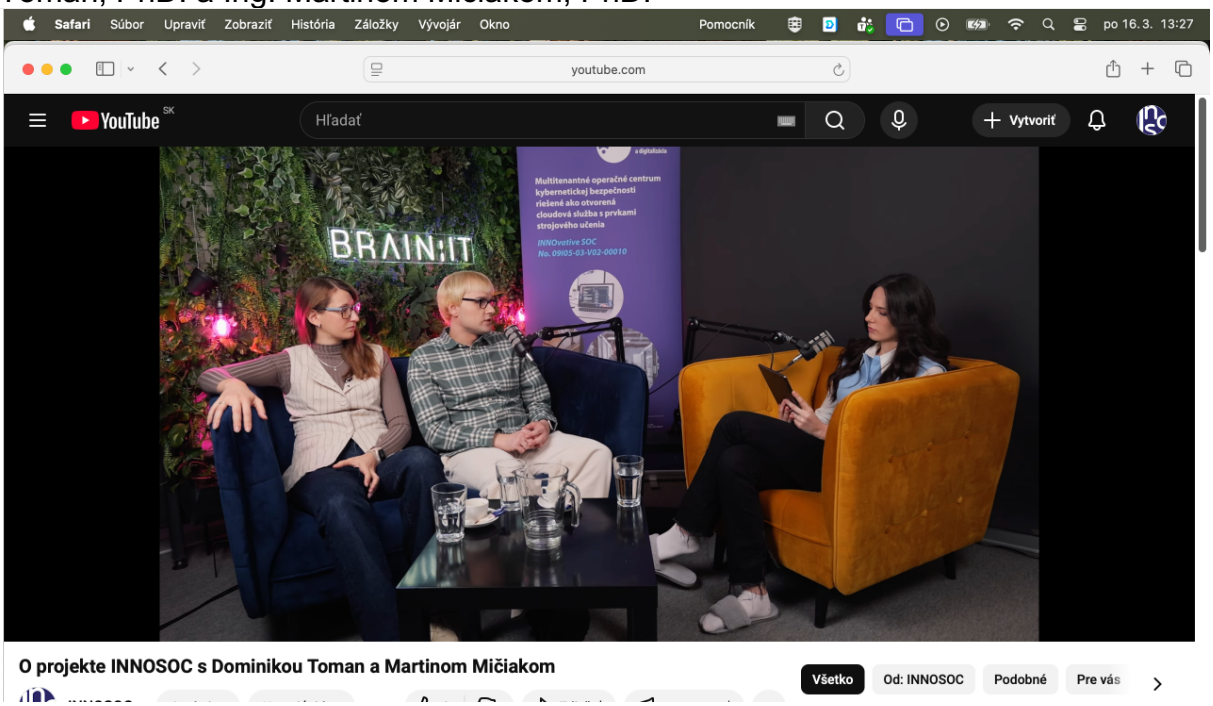
Praktické prínosy a výstupy:

- Pre podniky: Firmy získajú predpripravený návrh a prehľad komponentov, ktoré môžu využiť na posilnenie svojej bezpečnosti bez potreby budovať riešenie od nuly.

- Pre študentov: Projekt vytvára priestor pre záverečné práce a praktickú výučbu, kde si študenti môžu vyskúšať reálne situácie z projektového riadenia a IT praxe.
- Vedecká činnosť: Súčasťou projektu je publikačná činnosť v indexovaných časopisoch a účasť na konferenciách, čo si vyžaduje náročné plánovanie kvôli dlhým recenzným procesom.
- Riadenie rizík a výzvy: V rámci manažmentu sa tím musel vysporiadať s rizikami v komunikácii medzi viacerými partnermi a zladením časových harmonogramov (napríklad dovolenky na univerzite verzus projektové termíny). Náročné bolo aj priebežné monitorovanie a výkazníctvo pre grantové agentúry.
- Kľúčový výsledok: Za najvýznamnejší výstup hostia považujú proof of concept – reálne otestovanie navrhnutej architektúry, ktoré potvrdzuje, že riešenie je aplikovateľné v praxi a udržateľné pre koncových klientov.

Z hľadiska projektového manažmentu video vyzdvihuje najmä flexibilitu a iniciatívu členov tímu, ktorí dokázali úspešne reagovať na administratívne požiadavky a časový tlak.

Celý prepis rozhovoru sa nachádza v prílohe 24 – Rozhovor s Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD.



Obrázok 54: O projekte INNOSOC s Dominikou Toman a Martinom Mičiakom, Zdroj: (BRAIN:IT, 2026)

1.4.1.5 Videorozhovor s Ing. Martinom mičiakom, PhD.

Dňa 6. februára 2026 bolo na YouTube kanáli INNOSOC zverejnené video s názvom „Rozhovor s Ing. Martinom Mičiakom, PhD. o projekte INNOSOC“. Martin Mičiak v ňom približuje svoju dvojitú rolu v projekte – ako výskumný pracovník a zároveň ako súčasť podpory projektového riadenia. Hlavné body a témy rozhovoru zahŕňajú:

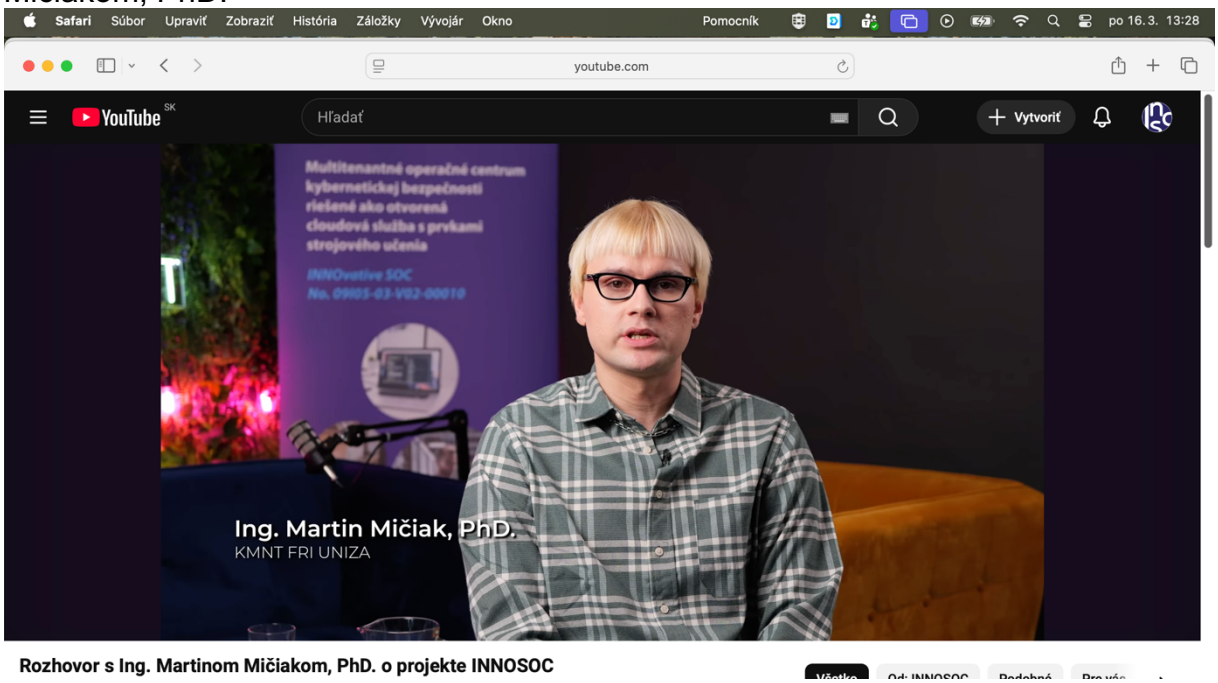
- Zameranie projektu: Témou projektu INNOSOC je kybernetická bezpečnosť s dôrazom na hľadanie možností, ako ju posilniť v organizáciách

prostredníctvom open-source riešení, čo vedie k zníženiu celkových nákladov.

- Vedecká a publikačná činnosť: Martin Mičiak zdôrazňuje, že pre relevanciu a šírenie povedomia o projekte je kľúčové publikovať výstupy v renomovaných vydavateľstvách a indexovaných časopisoch či na konferenciách.
- Výskumný proces: Za najnáročnejšiu časť označil samotný výskum a identifikáciu tzv. výskumnej medzery (research gap). Každý výstup musí prinášať niečo nové a detailne skúmať danú problematiku, aby bol zaujímavý pre odbornú komunitu aj prax.
- Interdisciplinárna spolupráca: Projekt je postavený na spolupráci akademického a biznis prostredia. V rámci fakulty ide o kooperáciu Katedry manažérskych teórií a Katedry informačných sietí, čo umožňuje efektívne prepojenie manažérskej a informatickej oblasti.
- Osobný prínos pre riešiteľa: Účasť na projekte umožnila Martinovi Mičiakovi prehĺbiť si vedomosti v téme kybernetickej bezpečnosti a získať ďalšie praktické skúsenosti z oblasti podpory projektového riadenia.

Tento rozhovor podčiarkuje akademický rozmer projektu a dôležitosť odborného výskumu, ktorý predchádza samotnej implementácii technických riešení do praxe.

Celý prepis rozhovoru sa nachádza v prílohe 25 – Rozhovor s Ing. Martinom Mičiakom, PhD.



Obrázok 55: Rozhovor s Ing. Martinom Mičiakom, PhD. o projekte INNOSOC, Zdroj: (BRAIN:IT, 2026)

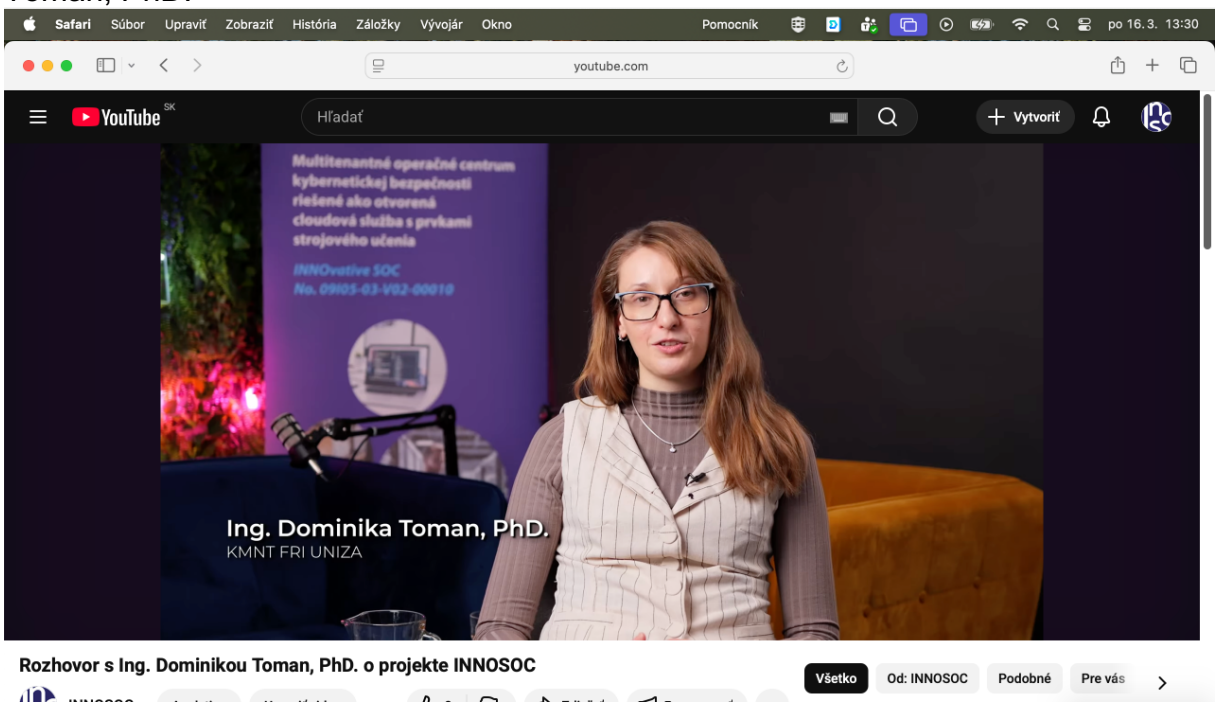
1.4.1.6 Videorozhovor s Ing. Dominikou Toman, PhD.

Dňa 6. februára 2026 bolo na YouTube kanáli INNOSOC zverejnené video s názvom „Rozhovor s Ing. Dominikou Toman, PhD. o projekte INNOSOC“. Dominika Toman v ňom približuje svoju rolu a kľúčové aktivity v rámci projektu. Hlavné body a témy rozhovoru zahŕňajú:

- Rola v projekte: Dominika Toman zabezpečuje predovšetkým podporu projektového riadenia a koordináciu ľudí zapojených do riešiteľského tímu.
- Význam projektu pre prax a verejnosť: Projekt vníma ako prostriedok na rozširovanie obzorov v kybernetickej bezpečnosti a poskytovanie informácií o tom, ako efektívne pomáhať v tejto oblasti. Z hľadiska odbornej praxe je kľúčové prehlbovanie znalostí prostredníctvom výskumu.
- Odborné výstupy a publikácie: V rámci projektu bolo publikované množstvo článkov a príspevkov na konferenciách, ktoré sa zameriavali na:
- Rešerše riešení: Identifikácia najvhodnejších technologických riešení pre podporu kybernetickej bezpečnosti.
- Vzdelávanie: Návrhy vhodných školení pre zamestnancov organizácií, aby dokázali nové riešenia správne ovládať a využívať na zlepšenie svojej bezpečnosti.
- Komunikácia s partnermi: Dôležitou súčasťou jej práce bola intenzívna komunikácia a spolupráca s partnermi priamo z univerzitného prostredia aj z reálnej praxe.
- Osobný a profesionálny rozvoj: Účasť na projekte riešiteľke umožnila získať nové informácie a zdokonaliť si zručnosti v oblasti riadenia a koordinácie výstupov.

Tento rozhovor zdôrazňuje, že projekt INNOSOC nie je len o technológiách, ale aj o dôležitosti manažérskej podpory a vzdelávania koncových používateľov, bez ktorých by implementácia kybernetickej bezpečnosti nebola efektívna.

Celý prepis rozhovoru sa nachádza v prílohe 26 – Rozhovor s Ing. Dominikou Toman, PhD.



Obrázok 56:Rozhovor s Ing. Dominikou Toman, PhD. o projekte INNOSOC, Zdroj: (BRAIN:IT, 2026)

1.4.1.7 Videorozhovor s prof. Ing. Milan Kubina, PhD.

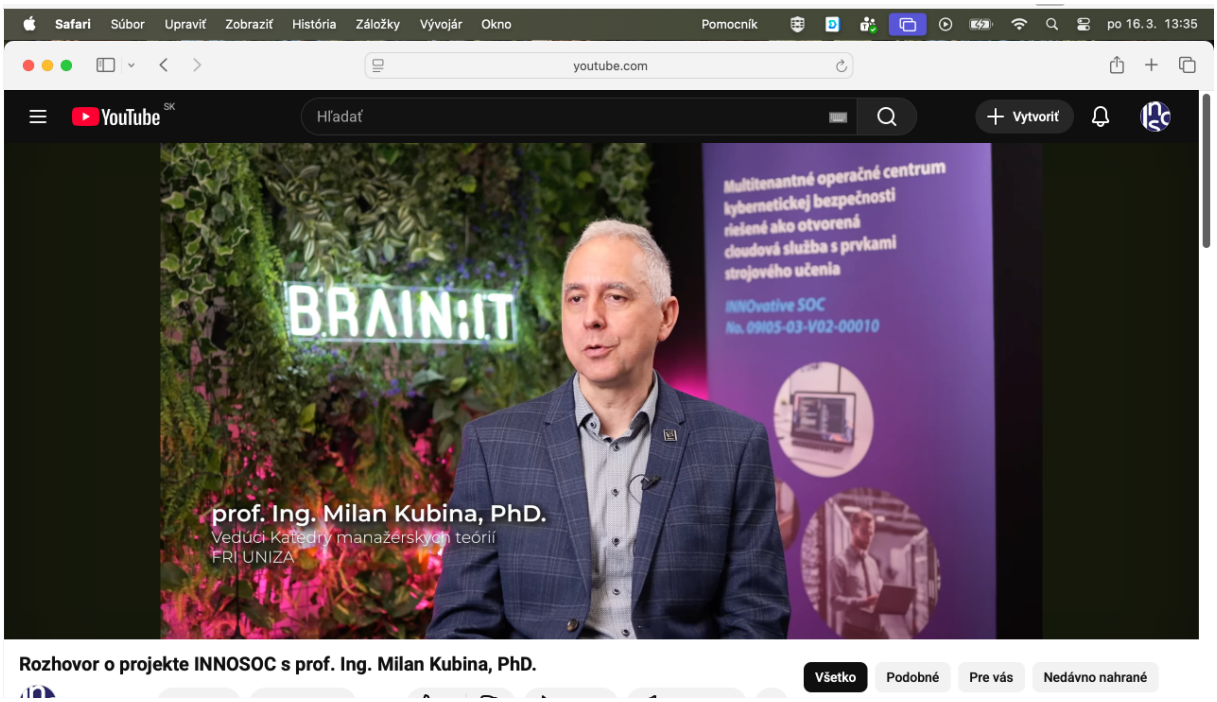
Pre potreby projektovej dokumentácie uvádzame súhrn informácií z rozhovoru s prof. Ing. Milanom Kubinom, PhD., vedúcim Katedry manažérskych teórií na Fakulte riadenia a informatiky UNIZA.

Dňa 20. februára 2026 bolo na YouTube kanáli INNOSOC zverejnené video s názvom „Rozhovor o projekte INNOSOC s prof. Ing. Milan Kubina, PhD.“. Rozhovor približuje strategické smerovanie projektu a jeho spoločenský význam. Kľúčové oblasti rozoberané v rozhovore zahŕňajú:

- Rola a zodpovednosť v projekte: Prof. Kubina vystupuje ako jeden z dvoch kľúčových zodpovedných riešiteľov (spolu s prof. Segečom). Jeho hlavnou úlohou je zabezpečenie komunikácie medzi jednotlivými výskumnými tímami, partnermi (najmä spoločnosťou BRAIN:IT) a grantovou vedeckou agentúrou.
- Spoločenský prínos a cieľová skupina: Projekt INNOSOC reaguje na riziká digitálnej doby, kde útočníci využívajú systémové chyby v aplikáciách. Riešenie je primárne určené pre subjekty, ktoré nemajú dostatok financií na drahé komerčné systémy – ide najmä o malé firmy, verejnú správu, obce a školy. Cieľom je, aby sa aj tieto organizácie cítili v kybernetickom priestore bezpečnejšie.
- Technické smerovanie a inovácie: Projekt sa zameriava na problematiku SOC (Security Operation Center) a bezpečnosť prevádzky IP sietí. Výstupom má byť návrh riešenia na úrovni TRL3, ktoré bude koncipované ako cloudová, multitenantná služba s dôrazom na nízku finančnú náročnosť pre budúcich odberateľov.
- Prepojenie univerzity s praxou: Prof. Kubina zdôrazňuje nevyhnutnosť synergie medzi akademickou sférou a reálnym biznisom. Túto spoluprácu podporuje nielen výskumom, ale aj motivovaním študentov k riešeniu praktických tém v rámci bakalárskych a diplomových prác či formou vyžiadaných prednášok odborníkov z praxe priamo na fakulte.

Tento rozhovor dopĺňa mozaiku projektu o pohľad vrcholového manažmentu výskumného tímu a podčiarkuje ambíciu vytvoriť dostupné technologické riešenie pre ochranu kritickej infraštruktúry menších organizácií.

Celý prepis rozhovoru sa nachádza v prílohe 27 – Rozhovor s prof. Ing. Milan Kubina, PhD.



Obrázok 57:Rozhovor o projekte INNOSOC s prof. Ing. Milan Kubina, PhD., Zdroj: (BRAIN:IT, 2026)

Zoznam zdrojov

BRAIN:IT. (16. október 2025). *innosoc.com*. Dostupné na Internete: Rozhovor s prof. Ing. Pavlom Segečom: https://innosoc.brainit.tech/kyberneticka-bezpecnost-uz-nie-je-len-temou-pre-velke-firmy/

BRAIN:IT. (2025). *innosoc.brainit.tech*. Dostupné na Internete: INNOSOS: https://innosoc.brainit.tech

BRAIN:IT. (11. november 2025). *innosoc.brainit.tech*. Dostupné na Internete: Študentská udalosť FRIčkovica: https://innosoc.brainit.tech/studentska-udalost-frickovica/

BRAIN:IT. (17. november 2025). *innosoc.brainit.tech*. Dostupné na Internete: Domov O projekte Výstupy Novinky Kontakt Sympózium – kybernetická bezpečnosť ako otvorená cloudová služba: https://innosoc.brainit.tech/sympozium-kyberneticka-bezpecnost-ako-otvorena-cloudova-sluzba/

BRAIN:IT. (24. november 2025). *innosoc.brainit.tech*. Dostupné na Internete: Súťaž o iPad: https://innosoc.brainit.tech/sutaz-o-ipad-vyhlasenie-vitaza/

BRAIN:IT. (28. november 2025). *innosoc.brainit.tech*. Dostupné na Internete: prezentácia na študentských raňajkách: https://innosoc.brainit.tech/prezentacia-projektu-innosoc-na-studentskych-ranajkach-4-november-2025/

BRAIN:IT. (9. december 2025). *innosoc.brainit.tech*. Dostupné na Internete: prezentácia na Univerzite Tomáše Báti v Zlíne: 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*. Dostupné na Internete: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v BB: https://innosoc.brainit.tech/prezentacia-na-strednej-priemyselnej-skole-jozefa-murgasa-v-banskej-bystrici-28-novembra-2025/

BRAIN:IT. (13. október 2025). *innosoc.brainit.tech*. Dostupné na Internete: Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska: https://innosoc.brainit.tech/co-je-to-cloud-ulozisko/

BRAIN:IT. (10. november 2025). *innosoc.brainit.tech*. Dostupné na Internete: Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady: https://innosoc.brainit.tech/pocitacova-bezpecnost-a-ochrana-dat/

BRAIN:IT. (2025). *innosoc.brainit.tech*. Dostupné na Internete: Článok: Rozhovor s odborníkmi: Ako projekt INNOSOC spája vedu, prax a kybernetickú bezpečnosť: https://innosoc.brainit.tech/rozhovor-s-odbornikmi-ako-projekt-innosoc-spaja-vedu-prax-a-kyberneticku-bezpecnost/

BRAIN:IT. (2025). *innosoc.brainit.tech*. Dostupné na Internete: Popularizačný článok na tému Prepojenie AI a kybernetickej bezpečnosti v praxi: https://innosoc.brainit.tech/ai-a-kyberneticka-bezpecnost/

BRAIN:IT. (2025). *innosoc.brainit.tech*. Dostupné na Internete: Popularizačný článok na tému Kybernetické útoky: Ako sa menia a prečo predstavujú čoraz väčšie riziko: https://innosoc.brainit.tech/kyberneticke-utoky-ako-sa-menia/

BRAIN:IT. (2025). *Instagram @brainit.tech*. Dostupné na Internete: príspevok webová stránka: https://www.instagram.com/p/DLXH_-MuL6_/

BRAIN:IT. (16. september 2025). *instagram @innosoc_*. Dostupné na Internete: kvíz o kybernetickej bezpečnosti: https://www.instagram.com/p/DOxr6HqiFeJ/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *Instagram @innosoc_*. Dostupné na Internete: príspevok zverejnený 5.9.2025: https://www.instagram.com/reel/DONouL4owoN/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *Instagram @innosoc_*. Dostupné na Internete: príspevok vo forme kvízu: https://www.instagram.com/p/DOV08sECMeh/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (2025). *Instagram @inosoc_*. Dostupné na Internete: príspevok stretnutie parterov 15.7.2025: https://www.instagram.com/p/DMpmaMAoMCj/?img_index=1

BRAIN:IT. (2025). *Instagram INNOSOC*. Dostupné na Internete: https://www.instagram.com/innosoc_/

BRAIN:IT. (3. október 2025). *instagramový účet @innosoc_*. Dostupné na Internete: súťaž o iPad: https://www.instagram.com/p/DPVvB7DiMUs/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==

BRAIN:IT. (3. október 2025). *instagramový profil @innosoc_*. Dostupné na Internete: súťaž o iPad: https://www.instagram.com/p/DPVvB7DiMUs/?utm_source=ig_web_copy_link&igsh=MWNyMTNjNWR2angwdg==
BRAIN:IT. (17. október 2025). *instagramový profil @innosoc_*. Dostupné na Internete: rozhovor s prof. Ing. Pavel Segeč, PhD.: https://www.instagram.com/reel/DP5wdgFiIav/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (18. november 2025). *instagramový profil @innosoc_*. Dostupné na Internete: oznam o konaní sympózia: https://www.instagram.com/p/DRMSZ4TiEZ9/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (24. november 2025). *instagramový profil @innosoc_*. Dostupné na Internete: odovzdávanie ceny súťaže: https://www.instagram.com/p/DRb0_wviDyq/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (28. november 2025). *instagramový profil @innosoc_*. Dostupné na Internete: prezentácia na študenstkých raňajkách: https://www.instagram.com/p/DRmQIOPiBFh/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (9. decembra 2025). *instagramový profil @innosoc_*. Dostupné na Internete: prezentácia na Univerzite Tomáše Báti v Zlíne: https://www.instagram.com/p/DSCxvhYiKGb/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (12. december 2025). *instagramový profil @innosoc_*. Dostupné na Internete: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici: https://www.instagram.com/p/DSKFfyniMg1/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2025). *Istagram @innosoc_*. Dostupné na Internete: príspevok z dňa 21.8.2025: https://www.instagram.com/reel/DNnIx9toFCU/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Dostupné na Internete: príspevok stretnutie partnerov 15.7.2025: https://www.linkedin.com/company/108018118/admin/page-posts/published/
BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Dostupné na Internete: príspevok zverejnený dňa 21.8.2025: https://www.linkedin.com/feed/update/urn:li:activity:7364224462050795520
BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Dostupné na Internete: príspevok zverejnený dňa 5.9.2025: https://www.linkedin.com/feed/update/urn:li:activity:7369610244873674752
BRAIN:IT. (2025). *LinkedIn @INNOSOC*. Dostupné na Internete: Popularizačný text na tému kybernetická bezpečnosť: https://www.linkedin.com/pulse/čo-je-kybernetická-bezpečnosť-innosocinnosoc-dt6we/?trackingId=cIrSBt0YN2qcFTrPUNfmvw%3D%3D
BRAIN:IT. (2025). *LinkedIn INNOSOC*. Dostupné na Internete: https://www.linkedin.com/company/innosocinnosoc/posts/?feedView=all
BRAIN:IT. (17. október 2025). *LinkedIn profil @innosoc*. Dostupné na Internete: rozhovor s 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 profil @innosoc*. Dostupné na Internete: oznam o konaní sympózia: https://www.linkedin.com/feed/update/urn:li:activity:7396442124268961792
BRAIN:IT. (24. november 2025). *LinkedIn profil @innosoc*. Dostupné na Internete: odovzdávanie ceny súťaže: https://www.linkedin.com/feed/update/urn:li:activity:7398667812409397248
BRAIN:IT. (9. december 2025). *LinkedIn profil @innosoc*. Dostupné na Internete: prezentácia na Univerzite Tomáše Báti v Zlíne: https://www.linkedin.com/feed/update/urn:li:activity:7404141474713325568
BRAIN:IT. (12. december 2025). *LinkedIn profil @innosoc*. Dostupné na Internete: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici: https://www.linkedin.com/feed/update/urn:li:activity:7405139422440071168
BRAIN:IT. (22. september 2025). *webová stránka INNOSOC*. Dostupné na Internete: Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany: https://innosoc.brainit.tech/najcastejsie-digitalne-hrozby-pre-mladych/

BRAIN:IT. (2025). *Webová stránka INNOSOC*. Dostupné na Internete: popularizačný článok na tému kybernetická bezpečnosť: Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami
BRAIN:IT. (2025). *Webová stránka INNOSOC*. Dostupné na Internete: Popularizačný článok: https://innosoc.brainit.tech/co-je-soc-security-operations-center/
BRAIN:IT. (2025). *YouTube @INNOSOC*. Dostupné na Internete: https://www.youtube.com/@INNOSOC
BRAIN:IT. (2025). *YouTube @INNOSOC*. Dostupné na Internete: video rozhovor s Ing. Michalom Papučíkom: https://youtu.be/w9W4_oNYiEQ?si=YlCKWgzX-JVkFZQK
BRAIN:IT. (15. október 2025). *YouTube @INNOSOC*. Dostupné na Internete: rozhovor s prof. Ing. Pavel Segeč, PhD.: https://www.youtube.com/watch?v=aKxL-Aig6sg
BRAIN:IT. (2026). *innosoc.brainit.tech*. Dostupné na Internete: Článok o rozhovore o projekte INNOSOC: Kybernetická bezpečnosť a rozširovanie obzorov s Dominikou Toman: https://innosoc.brainit.tech/rozhovor-o-projekte-innosoc-kyberneticka-bezpecnost-a-rozsirovanie-obzorov-s-dominikou-toman/
BRAIN:IT. (2026). *innosoc.brainit.tech*. Dostupné na Internete: Článok o rozhovore o projekte INNOSOC: O vedeckom výskume a kybernetickej bezpečnosti s Martinom Mičiakom.: https://innosoc.brainit.tech/rozhovor-o-projekte-innosoc-o-vedeckom-vyskume-a-kybernetickej-bezpecnosti-s-martinom-miciakom/
BRAIN:IT. (2026). *innosoc.brainit.tech*. Dostupné na Internete: článok o rozhovore s prof. Ing. Milanom Kubinom, PhD. o projekte INNOSOC: https://innosoc.brainit.tech/rozhovor-s-prof-ing-milanom-kubinom-phd-o-projekte-innosoc/
BRAIN:IT. (2026). *innosoc.brainit.tech*. Dostupné na Internete: Popularizačný článok na tému Automatizácia a hlboké strojové učenie v kybernetickej bezpečnosti: https://innosoc.brainit.tech/automatizacia-v-kybernetickej-bezpecnosti/
BRAIN:IT. (2026). *instagramový profil @innosoc*. Dostupné na Internete: Príspevok o rozhovore s Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD. na instagramovom profile @innosoc_: https://www.instagram.com/reel/DUnIqRnCN9A/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2026). *instagramový profil @innosoc_*. Dostupné na Internete: Príspevok o rozhovore s prof. Ing. Milanom Kubinom, PhD. na Instagramovom profile @innosoc_: https://www.instagram.com/reel/DVLEcgECOz5/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2026). *instagramový profil @innosoc_*. Dostupné na Internete: príspevok o rozhovore s Ing. Dominikou Toman, PhD. na instagrsamovom profile @innosoc_: https://www.instagram.com/reel/DUp1pl0CJvB/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
BRAIN:IT. (2026). *LinkedIn profil @innosoc*. Dostupné na Internete: príspevok o rozhovore s prof. Ing. Milanom Kubinom, 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*. Dostupné na Internete: Rozhovor s Ing. Martinom Mičiakom, PhD. o projekte INNOSOC: https://www.youtube.com/watch?v=UAtuHKnSQN0&t=2s
BRAIN:IT. (2026). *Youtube INNOSOC*. Dostupné na Internete: Rozhovor s Ing. Dominikou Toman, PhD. o projekte INNOSOC: https://www.youtube.com/watch?v=hY6lIE-UNh8
BRAIN:IT. (2026). *Youtube INNOSOC*. Dostupné na Internete: Rozhovor o projekte INNOSOC s prof. Ing. Milan Kubina, PhD.: https://www.youtube.com/watch?v=x6GnnEZXqHs
BRAIN:IT. (2026). *Youtube INNOSOC*. Dostupné na Internete: O projekte INNOSOC s Dominikou Toman a Martinom Mičiakom: https://www.youtube.com/watch?v=fhUuhltTAYY&t=198s

Prílohy

Prílohe 1 – Článok: Stretnutie partnerov 15.7.2025

Dňa 15. júla 2025 sa uskutočnilo ďalšie zo stretnutí stretnutie účastníkov projektu INNOSOC. Na stretnutí sa zúčastnili zástupcovia Fakulty riadenia a informatiky UNIZA a spoločnosti BRAIN:IT.
Na stretnutí sa zúčastnili zástupcovia Fakulty riadenia a informatiky UNIZA a spoločnosti BRAIN:IT.
Toto stretnutie bolo zamerané na diskusiu, ktorá sa týkala viacerých pracovných balíkov projektu:
ďalšie smerovanie vývoja projektu,
personálne zabezpečenie,
organizačné aspekty spolupráce počas letného obdobia.
V rámci stretnutia sa vyhodnotil aktuálny stav projektu po tom, čo bola odovzdaná priebežná monitorovacia správa. V aktuálnom momente sa ukončili analytické práce na 2.pracovných balíkoch, začínali sa vykonávať analytické štúdie potrebné pre 3. pracovný balík a experimentálne štúdie, aby sa získali dôkazy o technickej realizovateľnosti.
Vykonávali sa laboratórne testy na malých mierach a simulácie, kde sa zhromažďovali prvotné údaje o vlastnostiach technológie a potrebné bolo doladiť aj to, ako bude vyzerať samotná architektúra riešenia.
Otvorili sa témy:
Spracovanie a prístup k incidentom, ktoré sa na projekte vyskytujú.
Pracovné tímy si rozdelili úlohy a dohodli najbližšie individuálne aj spoločné kroky.
Zároveň sa načrtol plán výstupov a ich propagácie – pripravujú sa popularizačné príspevky, odborné články, a v budúcnosti aj videá či podcasty.

Príloha 2 – Článok: Základy projektu INNOSOC: Rozhovor s Ing. Michalom Papučíkom

Čo je projekt INNOSOC a aký je jeho cieľ?
Projekt INNOSOC je reakciou na rastúce požiadavky v oblasti kybernetickej bezpečnosti. Moderné prostredie si totiž vyžaduje pokročilé SaaS a cloudové služby, ktoré dokážu efektívne reagovať na nové hrozby. A na základe čoho vznikol názov INNOSOC?
Innovative and Security Operation Center – to sú slová, ktoré reprezentujú skratku INNOSOC a ak vás zaujíma prečo práve takýto názov, vypočujte si celé video, kde Ing. Michal Papučík, COO spoločnosti BRAIN:IT, odpovedá aj na ďalšie zaujímavé otázky, ktoré sa týkajú základov projektu.
Čo sa vo videu dozviete?
Čo je projekt INNOSOC a prečo vznikol.
Čo reprezentuje názov INNOSOC.
Aký je cieľ projektu.
Na aký problém alebo výzvu reaguje.
Aké prínosy môže projekt priniesť.
Čo ho na projekte najviac baví.
S akými technológiami tím pracuje.
Akú úlohu v projekte zohráva spoločnosť BRAIN:IT.
Ako sa darí prepájať akademickú a biznis sféru.
Aké metódy a medzinárodné štandardy sa využívajú.

Ak vás o projekte INNOSOC zaujíma viac, pozrite si celý rozhovor s Michalom Papučíkom vo videu nižšie.

Príloha 3 – Článok: Rozhovor s prof. Ing. Pavlom Segečom, PhD.: Kybernetická bezpečnosť už nie je len témou pre veľké firmy

V rámci projektu INNOSOC – Innovative & Security Operations Center sme sa rozprávali s prof. Ing. Pavlom Segečom, PhD., vedúcim Katedry informačných sietí na Fakulte riadenia a informatiky UNIZA.
Profesor Segeč je kľúčovým vedecko-výskumným pracovníkom projektu, ktorý sa zameriava na posilnenie kybernetickej bezpečnosti v organizáciách a školách prostredníctvom inovatívnych technológií a vzdelávania novej generácie odborníkov.
Kybernetická bezpečnosť sa týka každého?
Na úvod rozhovoru prof. Segeč vysvetľuje, prečo je bezpečnosť IT infraštruktúry aktuálnou témou aj pre malé organizácie:
„Kybernetická súčasnosť v súčasnosti je za mňa kľúčovou témou, pretože žijeme v dobe, kedy je všetko poprepájané a sme v online svete a siete sa stávajú digitálnymi diaľnicami, ktoré umožňujú a podporujú naše správanie, biznis a ďalšie aspekty nášho života.“
Úloha Fakulty riadenia a informatiky UNIZA v projekte INNOSOC
Fakulta riadenia a informatiky (FRI) je jedným z hlavných partnerov projektu a zastrešuje vedecko-výskumnú časť aj vývojové aktivity.
„V rámci projektu INNOSOC poskytujeme svoje kapacity, zároveň poskytujeme svoju privátnu infraštruktúru ako koncept, na ktorom je možné robiť pilotné nasadenia technológií, ktoré sú v projekte,“ hovorí profesor Segeč.
Najčastejšie hrozby a potreba centralizovanej ochrany
Medzi najčastejšie hrozby podľa štatistických údajov patria phishingové útoky, ransomvér alebo APT (Advanced Persistent Threat), kedy útočník dlhodobo vykonáva špionáž a monitorovanie v sieti obete.
Security Operations Center (SOC) ako jadro obrany
Jedným z hlavných výstupov projektu INNOSOC je návrh a budovanie Security Operations Centra (SOC) – centrálneho uzla, ktorý monitoruje, analyzuje a reaguje na kybernetické incidenty v reálnom čase.
„SOC centrá stavajú na troch pilieroch, to sú ľudia, procesy a technológie,“ dopĺňa prof. Segeč.
Nové požiadavky prináša smernica NIS2
V rozhovore sa venoval aj pripravovanej implementácii smernice NIS2, ktorá zásadne mení požiadavky na kybernetickú ochranu v celej EÚ.
„Vďaka NIS2 smernici, ktorá bola transponovaná do slovenskej legislatívy sa sprísnili požiadavky na zvýšenie úrovne bezpečnosti a riadenia bezpečnosti v spoločnostiach. Zároveň aj aspekty, ktoré sú spojené s reportovaním útokov a práve to reportovanie útokov a ich odhaľovaniu by mali pomôcť SOC centrá.“
Ako fungujú SOC systémy
Na záver profesor priblížil, ako takéto systémy fungujú v praxi:
„SOC centrá technologicky fungujú na princípe telemetrického zberu veľkého množstva údajov, kde tieto údaje sú následne vkladané do databáz a obohacované o rôzne doplnkové údaje za účelom ľahšej detekcie a odhalenia anomálneho správania.„

Celý rozhovor s prof. Ing. Pavlom Segečom, PhD. si môžete pozrieť vo videu nižšie. Vysvetľuje v ňom, prečo kybernetická bezpečnosť nie je len technická téma, ale nevyhnutný základ pre dôveryhodné a stabilné fungovanie organizácií.

Príloha 4 – Článok: Študentská udalosť FRIčkovica – 8.októbra

Dňa 8. októbra sa na Fakulte riadenia a informatiky konala tradičná každoročná udalosť – FRIčkovica, ktorá je miestom neformálneho stretnutia študentov, vyučujúcich a partnerov fakulty.
V rámci konania podujatia bol pre študentov prichystaný aj stánok na propagáciu výskumného projektu INNOSOC. Počas komunikácie so študentami tak boli predstavené highlighty projektu, napríklad jeho zámer, ciele a problémy, ktoré rieši. Prezentácia študentom ukázala význam projektu aj jeho prínosy. Cieľom prezentácie na študentskej akcii bolo priniesť mladým odborníkom bližšie poznatky z oblasti kybernetickej bezpečnosti.

Príloha 5 – Oznam o konaní sympózia INNOSOC

Dňa 18.12.2025 sa uskutoční sympózium na tému kybernetická bezpečnosť ako otvorená cloudová služba v rámci projektu INNOSOC. Sympózium sa bude konať v priestoroch Žilinskej univerzity v Žiline v prednáškovej miestnosti Aula AF3A5 od 8:00 do 10:45.
Počas sympózia bude prezentovaný súčasný stav a výsledky výskumného projektu.

Príloha 6 – Článok o vyhlásení víťaza súťaže o iPad

Dňa 10. novembra 2025 bola ukončená súťaž o iPad, ktorá bola organizovaná prostredníctvom instagramového profilu @innosoc_. Cieľom súťaže bolo zapojiť mladých študentov a vzbudiť u nich záujem o projekt INNOSOC a oblasť kybernetickej bezpečnosti.
Po oficiálnom losovaní sa víťazom súťaže stal Timotej Djubašák, ktorý splnil všetky podmienky a výhru si osobne prebral.
Gratulujeme výhercovi.

Príloha 7 – Článok: Prezentácia projektu INNOSOC na študentských raňajkách

Dňa 4. novembra 2025 sa na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline konali študentské raňajky v spolupráci so spoločnosťou BRAIN:IT, v rámci ktorých sa prezentoval projekt INNOSOC mladým študentom z manažérskych a informatických odborov.
Študenti mali možnosť v rámci neformálneho podujatia získať informácie o projekte, dozvedieť sa o aktuálnom stave, výstupoch a ďalších postupoch.
Rovnako tak boli prezentované dôležitosti kybernetickej bezpečnosti, význam Security Operation Centra a cloudových technológií.

Príloha 8 – Článok o prezentácii projektu na fakulte Aplikovanej informatiky na Univerzite Tomáše Báti v Zlíne

Dňa 20.novembra 2025 sa študentom fakulty Aplikovanej informatiky na Univerzite Tomáše Bati v Zlíne prezentoval projekt INNOSOC. Zástupcom projektu, ktorý o projekte na fakulte rozprával bol Ing. Michal Papučík.
Prezentácia projektu bola zameraná najmä na bližšie predstavenie toho, ako projekt pomáha a reflektuje na výzvy spojené s prechodom na digitálnu ekonomiku. Ing.

Michal Papučík zároveň hovoril aj o potrebách komerčnej sféry, o dopyte po moderných IT službách, potrebe posunúť spoločnosť na vyššiu úroveň bezpečnosti a o potrebe IT špecialistov.
Študenti sa zároveň mohli dozvedieť o princípoch a technológiách, ktoré sa pri projekte využívajú.

Príloha 9 – Článok o prezentácii projektu INNOSOC na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici

Dňa 28. novembra sa konala prezentácia projektu INNOSOC na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici.
V rámci prezentácie sa žiaci dozvedeli:
O čo v projekte ide.
Čoho sa projekt INNOSOC týka.
Aké typy útokov v dnešnej dobe poznáme.
Aké základné školy sa na projekte podieľajú.
Prečo je kybernetická bezpečnosť dôležitá.
Celá prezentácia bola interaktívna a pri prezentácii išlo aj o aktívne zapojenie mladých žiakov do problematiky.

Príloha 10 – Článok: Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami

Čo je kybernetická bezpečnosť?
Kybernetická bezpečnosť (angl. cybersecurity) označuje súbor opatrení, technológií a procesov, ktorých základným cieľom je chrániť počítače, servery, siete a programy pred neoprávneným prístupom, zneužitím alebo poškodením, teda pred kybernetickými hrozbami a útokmi. Ochranu potrebujú najmä dáta, informácie a údaje, ktoré sa nachádzajú v týchto zariadeniach.
Ľudia, ktorí stoja za kybernetickými útokmi, sú hackeri. Snahou tejto skupiny ľudí je získať prístup do vašich zariadení, systémov a sietí s cieľom odcudziť z nich citlivé osobné údaje, prípadne aj iné kompromitujúce materiály. S týmito dátami, informáciami a obsahom následne hackeri obchodujú, predávajú ich alebo ich využívajú na vydieranie poškodených osôb.
Hackeri sú pritom často veľmi dobre vybavení rôznymi IT zručnosťami a neraz disponujú najmodernejšími technológiami. Preto je dôležité, aby ste sa pravidelne starali o svoje údaje, systémy, siete a zariadenia a dostatočne ich chránili pred zneužitím.
Ochrana sa v praxi týka najmä týchto dvoch základných faktorov:
Ľudský faktor
Táto oblasť zahŕňa dodržiavanie základných zásad ochrany osobných údajov a súkromia. V praxi to znamená, že dbáte na to, aké údaje o vašej práci a súkromí zdieľate s inými, na akých platformách a akou formou. Tento segment zahŕňa aj obozretnosť pri používaní hesiel, otváraní podozrivých správ a e-mailov, prijímaní podozrivých telefonátov, ako aj pri klikaní na rôzne neoverené stránky.
Technologický faktor
Hackeri majú pred vami často náskok nielen vďaka svojim rozvinutým IT zručnostiam, ale disponujú aj modernými a pokročilými technológiami. V praxi preto môže pomôcť, ak sú vaše technológie novšie alebo aspoň pravidelne aktualizované. Staré technológie niekedy neumožňujú používanie nových a sofistikovaných ochranných

prvkov. Kľúčovú ochranu v prípade technológií zohráva kvalitný a pravidelne aktualizovaný antivírus a firewall.

Prečo je kybernetická bezpečnosť dôležitá?

Kybernetické hrozby na vás číhajú doma aj v práci a ich zákernosť spočíva najmä v tom, že dokážu ohroziť vaše citlivé miesta a v tom najhoršom prípade aj celú vašu existenciu. Kybernetická bezpečnosť vám pomáha chrániť sa pred zneužitím osobných a firemných údajov.

Ohrozené informácie

Osobné a kontaktné údaje týkajúce sa vašej identity, ako je meno, priezvisko, rodné číslo a ďalšie osobné údaje, ako aj vaše kontaktné údaje (telefón, e-mail, adresa a iné)
Zdravotné údaje a informácie o vašom fyzickom a psychickom zdraví
Finančné údaje, údaje o úveroch a podobné citlivé informácie
Údaje o osobnom stave, manželoch, deťoch a iných rodinných príslušníkoch
Všetky vyššie uvedené informácie, heslá, čísla účtov, osobné dáta a údaje o pracovných aktivitách a firmách môžu byť zneužité a môžu vám privodiť rôzne fyzické, materiálne, finančné aj psychické ujmy.

Základné zásady kybernetickej bezpečnosti

Množstvo osobných a pracovných aktivít prebieha online. Spolu s tým rastie aj dôležitosť kybernetickej bezpečnosti a potreba ochrany v tomto segmente. Od bežných ľudí až po veľké korporácie je každý človek vystavený potenciálnym kybernetickým útokom, pričom citlivé skupiny tvoria najmä deti a starší ľudia.
Dodržiavanie zásad kybernetickej bezpečnosti vám môže významne pomôcť znížiť pravdepodobnosť zneužitia a krádeže údajov.

Faktory kybernetickej bezpečnosti:

Silné a unikátne heslá: Používanie kombinácie veľkých a malých písmen, čísel a špeciálnych znakov. Pre každú službu si nastavte iné silné a jedinečné heslo.
Dvojfaktorová autentifikácia (2FA): Tento postup pridáva ďalšiu vrstvu ochrany pri prihlasovaní sa do vašich technologických zariadení a rôznych účtov.
Pravidelné aktualizácie: Pravidelné aktualizácie udržiavajú váš operačný systém a aplikácie aktuálne a pri mnohých sa inovujú a vylepšujú aj rôzne ochranné prvky.
Zálohovanie dát: Pravidelná záloha dôležitých údajov, informácií a dokumentov na externé disky a/alebo cloud tiež prispieva k ochrane vašich údajov.
Ostražitosť pri e-mailoch a odkazoch: Neklikajte na podozrivé odkazy ani prílohy od neznámych odosielateľov. Sledovanie rôznych podvodov a techník hackerov tiež významne prispieva k väčšej informovanosti o potenciálnych hrozbách a rizikách. Väčšina týchto podvodov je založená na vašej nepozornosti. Vedomá pozornosť, opatrnosť a overovanie si faktov pomáha aj v tejto oblasti.
Antivírus a firewall: Tieto nástroje patria do základnej výbavy každého zariadenia a každého, kto pôsobí v online priestore. Urobia pre vás veľkú prácu v oblasti ochrany pred nabúraním sa do vašich systémov, sietí a technologických zariadení.

Najčastejšie typy kybernetických hrozieb

Zachovať si bezpečnosť v online prostredí môže byť náročné, ale pri dodržiavaní základných zásad kybernetickej bezpečnosti a vašej vedomej pozornosti je to možné. Je pritom dobré vedieť aj to, aké potenciálne a reálne riziká existujú a čo vás môže ohrozovať.
Prinášame vám niektoré z nich, s ktorými sa bežne môžete stretnúť:
Phishing: Podvodné e-maily alebo správy, ktoré sa snažia získať citlivé údaje.

Malvér (škodlivý softvér): Vírusy, trójske kone, ransomvér (ransomware). Všetky tieto vírusy môžu poškodiť vaše zariadenie a ukradnúť vaše dáta.
Útoky hrubou silou (brute force): Automatizované pokusy uhádnuť heslá do vašich systémov, účtov a aplikácií.
Sociálne inžinierstvo: Manipulácia ľudí s cieľom získať od vás dôverné informácie.
DDoS útoky: Preťaženie servera s cieľom znefunkčniť určitú službu alebo celý web.
XSS (Cross-Site Scripting): Kybernetický útok na webové aplikácie, pri ktorom hackeri vkladajú škodlivé skripty priamo na webovú stránku.

Myslite na prevenciu

Základy kybernetickej bezpečnosti sú dnes rovnako dôležité ako zamykanie dverí od bytu alebo domu. Čím viac budete o tejto problematike vedieť, tým lepšie sa ochránite pred zvyšujúcimi sa digitálnymi hrozbami a potenciálnymi kybernetickými rizikami. Prevencia je aj v tomto segmente jednoduchším a neraz aj lacnejším riešením ako následné komplikované napravovanie spôsobených škôd.

Príloha 11 – Článok: Security Operations Center: čo to je a ako chráni vašu firmu?

Čo je Security Operations Center (SOC)?

S príchodom digitalizácie sa stále častejšie stretávame aj s rôznymi kybernetickými hrozbami a bezpečnostnými rizikami ohrozujúcimi jednotlivcov a organizácie. Kybernetická bezpečnosť pritom predstavuje súbor opatrení, ktorých cieľom je chrániť digitálne systémy, siete, procesy a programy pred krádežou údajov alebo iným narušením prevádzky organizácie. Security Operations Center reprezentuje v tomto smere výkonný článok, ktorého cieľom je reálna ochrana týchto dát.
Security Operations Center (SOC) je špecializované stredisko, ktoré vykonáva nepretržitý monitoring bezpečnosti v organizácii a reaguje na reálne kybernetické hrozby a incidenty. SOC je centralizovaná jednotka alebo tím odborníkov, ktorí non-stop zabezpečujú sledovanie a vyhodnocovanie potenciálnych kybernetických hrozieb v reálnom čase.

Čo je hlavnou úlohou SOC?

Základnou úlohou Security Operations Center je minimalizovať dopad bezpečnostných incidentov a kybernetických útokov na organizáciu a proaktívne zaisťovať jej kybernetickú a inú bezpečnosť podľa potreby a dohody.

Ako pracuje SOC?

Pracovný tím Security Operations Center väčšinou tvoria bezpečnostní analytici a IT odborníci, ktorí pracujú s pokročilými technológiami. Tieto technológie pomáhajú chrániť digitálne a iné aktíva organizácie.

Aké modely SOC sa využívajú v praxi?

V praxi môžeme nájsť dva základné modely Security Operational Center. V prvom prípade vykonáva hlavné funkcie strediska interná organizácia, respektíve na to určené oddelenie danej organizácie. V druhom prípade sú tieto právomoci zverené do rúk externému subjektu. Často sa využíva aj kombinácia oboch modelov.

Aké sú hlavné funkcie Security Operations Center?

Security Operations Center zaisťuje pre organizácie nasledovné hlavné funkcie:
Monitorovanie a detekcia incidentov
V rámci tejto funkcie SOC zabezpečuje monitorovanie systémov a sietí 24/7. Vyhľadáva pritom podozrivú aktivitu pomocou bezpečnostných nástrojov, ktoré sledujú sieťovú prevádzku a aktivitu zariadení.
Riadenie incidentov

Táto funkcia centra je využívaná po identifikovaní bezpečnostného incidentu a zahŕňa napríklad nasledovné činnosti:
zhromažďovanie informácií, ktoré prispievajú k pochopenie rozsahu a typu incidentu,
prijatie nápravných opatrení, ako je izolácia alebo eliminácia rizika s cieľom čo najviac znížiť negatívny dopad incidentu a predísť jeho opakovaniu,
vyšetrovanie základnej príčiny incidentu s cieľom zistiť jeho zdroj a zaviesť potrebné kontroly na obmedzenie akýchkoľvek bezpečnostných medzier do budúcnosti,
overenie, či bol incident riadne zdokumentovaný a vyriešený, ako aj kontrola, či sú všetky relevantné procesy aktualizované.
Riadenie problémov
V rámci tejto aktivity sa Security Operations Center zameriava najmä na hlbšie pochopenie príčin kybernetických a iných bezpečnostných incidentov s cieľom eliminácie rovnakých alebo podobných problémov v budúcnosti. Neraz pritom úzko spolupracuje aj s danou organizáciou, prípadne tvorí jej interný tím.

Odporúčania na záver

Security Operational Center môže poskytovať aj ďalšie bezpečnostné služby, ktoré daná organizácia potrebuje. Každá organizácia by sa preto už v súčasnosti mala zaoberať aj otázkou kybernetickej bezpečnosti a zaisťovaním bezpečnosti citlivých údajov, procesov, informácií, systémov, sietí a používaných zariadení.
Každá organizácia by si mala vytvorila svoju vlastnú internú politiku a postupy, ktoré zahŕňajú údaje a oblasti vystavené potenciálnej krádeži alebo inému kybernetickému útoku, zneužitiu alebo bezpečnostnej hrozbe. V rámci tohto postupu odporúčame:
nastavenie procesov v oblasti monitoringu,
nastavenie eskalačných postupov,
nastavenie možností reakcie na reálne incidenty,
personálne zabezpečenie,
iné nastavenie s ohľadom na praktické potreby a požiadavky konkrétnej organizácie a jej aktuálnu situáciu.
Za týmto účelom si môžete vytvoriť svoje vlastné interné smernice, šablóny a procesy, ktoré vám pomôžu efektívne chrániť citlivé údaje, informácie a zariadenia.

Príloha 12 – Článok: Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany

Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany

Súčasná generácia vyrastá v tzv. informačnom a technologickom veku, kedy sú súčasťou ich každodenného života rôzne technológie a bežným statusom qou je aj pohyb v online priestore. Nástroje im umožňujú jednoduchý prístup do digitálneho sveta, kde komunikujú, vyhľadávajú informácie, vzdelávajú sa a zabávajú.
V online priestore sa šíria aj potenciálne hrozby, ktoré na mladých číhajú. Aby sa dokázali efektívne brániť pred týmito rizikami mali by vedieť o tom, čo im hrozí a oboznámiť sa s tým, ako sa možno voči týmto hrozbám chrániť. Prečítajte si o najčastejších nástrahách, prevencii a ochrane voči nim.

Hrozby a riziká digitálneho sveta pre mladých

Potenciálne hrozby už dávno nečíhajú na mladých len za bránami vašich domovov. Často sú k nim oveľa bližšie a rafinovanejšie, ako si dokážete predstaviť. Oblasť digitálneho sveta je relatívne novým územím aj pre mnohých dospelých. Ak chcete účinne chrániť mladých pred digitálnymi hrozbami, jednou z ciest je aj pravidelné

vzdelávanie sa o rizikách a bezpečnosti v online priestore. Prevencia je základom úspechu aj v tejto oblasti.
Technologický vývoj napreduje dynamickým tempom, a preto je niekedy veľmi ťažké rozpoznať riziká.
Pozrite si prehľad najčastejších hrozieb v digitálnom svete, ktoré ohrozujú nielen mladých.
Vyhľadávanie (surfovanie) na internete
Internet je významným zdrojom veľkého množstva rôznorodých informácií, ktoré môžu mať ďalekosiahly negatívny dopad na mladých. Mladí často ešte nevedia účinne rozlíšiť, čo je urážlivý, toxický a nebezpečný obsah a nevedia často ani to, ako bezpečne vyhľadávať požadované informácie na internete a kam radšej neklikať.
Obsah pre dospelých
Ďalšou veľkou hrozbou nielen pre mladých je jednoduchá a rýchla dostupnosť obsahu pre dospelých na internete. Tento obsah je pre nich často nielen nevhodný, ale v mnohých ohľadoch aj reálne nebezpečný.
Komunikácia na sociálnych sieťach
Ani mnohí rodičia a iní dospelí ešte stále nemajú dostatočné povedomie o tom, aké hrozby sú prítomné v online priestore a bez väčšieho zamyslenia sa bežne zverejňujú svoje citlivé údaje, informácie, fotky seba a svojich detí a podobne. Je veľmi dôležité, aby ste sa naučili efektívne chrániť svoje súkromie a učili to aj svoje deti.
Komunikácia intímnych záležitostí a posielanie intímneho obsahu
Samostatnou kapitolou v rámci komunikácie je posielanie správ, fotografií alebo iného intímneho obsahu. Ak je takýto obsah nejakým spôsobom zneužitý, tak následky nesú mladí ľudia často po celý život. Takýto obsah a informácie sú ľahko zneužiteľné mnohými spôsobmi na vydieranie a inú nelegálnu a trestnú činnosť.
Internetové podvody
Mladí nakupujú na internete. Je to pohodlné a často aj lacnejšie. S väčším dopytom však rastie aj chuť podvodníkov, ktorí používajú pri svojich online podvodoch stále sofistikovanejšie metódy. Pri týchto podvodoch môžu užívatelia prísť o svoje osobné údaje, ktoré môžu byť zneužité, peniaze, súkromie a iné.
Medzi ďalšími hrozbami je aj riziko, že mladí môžu podľahnúť hrám a gamblingu, riziko spojené s diskrimináciou, rôzne typy šikany, vydierania a zneužívania, ako aj stretnutie sa s rôznymi nenávistnými prejavmi.
Nezanedbateľným rizikom je aj vznik závislosti od technológií, sledovania sociálnych sietí a internetových vzťahov, ktoré prehlbujú strach z premeškania (FOMO), strach z lepších možností (FOBO) a vedú k psychickým ťažkostiam či sociálnej izolácii.

Bezpečnostné odporúčania a ochrana mladých

Digitálny svet je súčasťou nášho každodenného života. Mali by ste sa v ňom naučiť bezpečne pohybovať a odovzdať tieto princípy mladým. Je dôležité rozumieť tomu, že takéto nebezpečenstvo existuje a je ťažko rozpoznateľné. Naučte sa ho rozpoznať a účinne aplikovať možnosti ochrany.
Zodpovednosť za to, aké údaje a obsah zverejňujete na internete, sociálnych sieťach a iných komunikačných weboch a platformách. Detaily, ako je adresa bydliska a telefónne čísla verejne nezdieľajte.
Platí to aj o údajoch a informáciách o tom, kde pravidelne chodievate, čo tam robíte, s kým a tak podobne.
Zdieľanie fotografií je veľmi populárne. Táto činnosť však v sebe nesie veľké riziko potenciálneho zneužitia rôznymi spôsobmi. Ak sú na obrazoch a fotografiách zobrazené odhalené telá mladých, alebo vo vyzývavých pózach, tak sa hrozba ešte

zvyšuje. Nahé fotografie malých detí by určite mali zostať súčasťou rodinných albumov.Nie je to obsah, ktorý by ste mali ukazovať komukoľvek inému.
Interakcia s ľuďmi, ktorých nepoznáte. Internet poskytuje anonymitu pre ľudí a s absolútnou istotou nikdy neviete, s kým komunikujeme. Nekomunikovať s cudzími ľuďmi a nenasledovať ich je v online priestore snáď ešte zásadnejšou formou prevencie a ochrany, ako vo fyzickom svete.

Bezpečný svet začína u vás doma

Buďte vzorom a komunikujte s mladými o hrozbách v digitálnom svete otvorene. Vytvorte im domov, v ktorom nebudú musieť hľadať vzťahy, informácie a zábavu niekde inde. Keď sú mladí vychovávaní v bezpečnom, láskavom, inšpiratívnom a podnetnom prostredí, v ktorom majú možnosť autenticky sa prejavovať a sú v tom podporovaní, tak je to základná prevencia pred mnohými problémami a hrozbami. Budujte v deťoch zdravé hranice.

Príloha 13 – Článok: Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska

Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska

Cloud je termín, ktorý označuje dátové úložisko, prostredníctvom ktorého môžu používatelia zdieľať, ukladať alebo inak manipulovať s veľkým množstvom informácií a údajov. V tomto článku vám jednoducho vysvetlíme, čo je to cloud a na čo vám v praxi môže poslúžiť. Okrem toho vám priblížime aj základné výhody a nevýhody využívania cloudových služieb.

Čo je to cloud a na čo slúži?

Cloud, nazývaný aj cloudové úložisko, je online služba, ktorá umožňuje ukladať, uchovávať a spravovať vaše dáta, ako sú rôzne osobné alebo firemné súbory, dokumenty, fotografie a videá. Vaše dáta sa takto ukladajú na cloudové servery pripojené k internetu, ktoré sú umiestnené na rôznych miestach po celom svete v dátových centrách. Cloud je služba, ktorú môžu kedykoľvek využívať firmy alebo jednotlivci cez platený prenájom, alebo ako súčasť softvéru či platformovej služby.

Formy cloudových služieb

Služby založené na cloude môžu mať veľa rôznych foriem, ako napríklad nasledovné:
Web hosting.
Zdieľanie súborov.
Distribúcia softvéru a iných služieb.
Ukladanie a uchovávanie súborov, fotografií, videí, osobných a firemných dokladov, dokumentov, zmlúv, zamestnaneckých, obchodných či iných prevádzkových údajov, projektov a iných potrebných informácií.
Cloud computing, ktorý označuje metódu používania niekoľkých navzájom prepojených serverov s cieľom zdieľať pracovné aktivity, projektov alebo iných špecifických úloh.

Základné typy cloudov (cloudových úložísk)

Medzi základné typy cloudov patrí verejný, súkromný a hybridný cloud. Nižšie vám v krátkosti predstavíme ich základné funkcie.
Verejný cloud (Public cloud)
Je to zdieľaná infraštruktúra prevádzkovaná externým poskytovateľom služieb. Vaše dáta sú v takomto prípade uložené v dátových centrách externého poskytovateľa, ktoré sa môžu nachádzať kdekoľvek na svete. Poskytovateľ cloudovej služby je pritom

zodpovedný za celkovú prevádzku a komplexný manažment cloudového prostredia vrátane hardvéru, softvéru a celého dátového centra. Zákazník, ktorý si väčšinou prenajíma príslušný úložný priestor, je v tomto prípade len používateľom služby.
Poznámka:
To, že je cloud verejný, však neznamená, že k uloženým dátam má prístup ktokoľvek. Zákazník môže napríklad ustanoviť, že jeho infraštruktúra je dostupná len pre jeho rodinu, zamestnancov či partnerov firmy. Nikto iný sa k uloženému obsahu, dátam a informáciám nedostane.
Súkromný cloud (Private cloud)
Ide o priestor, ktorý sa nachádza v dátovom centre samotnej spoločnosti. V tomto prípade si cloud prevádzkuje, manažuje, spravuje a udržiava samotná firma vo vlastnej réžii. Takéto riešenie je v praxi väčšinou o niečo drahšie a vyžaduje si extra náklady vynaložené na potrebnú odbornú pracovnú silu, hardvér aj softvér.
Hybridný cloud (Hybrid cloud)
Predstavuje kombináciu oboch vyššie uvedených modelov. Časť služieb je v týchto prípadoch prevádzkovaná na verejne dostupnej infraštruktúre u externého poskytovateľa a časť služieb je uložená na súkromnom cloude spoločnosti. Na súkromnom cloude sú väčšinou uložené citlivé údaje firmy a je pritom vyšpecifikovaný aj prístup k týmto údajom alebo jednotlivým úrovniam u konkrétnych pracovníkov firmy alebo iných ľudí.
Výhody a nevýhody cloudových služieb
Medzi nesporné výhody cloudu patrí vyššia produktivita, ktorá je možná vďaka rýchlemu toku a cirkulácii údajov, dokumentov a informácií. Zdieľanie zdrojov spravidla vedie k vyššej efektivite vo firemných procesoch a tým sa znižujú aj náklady na zamestnancov a iné pracovné úkony. K znižovaniu nákladov napokon prispieva aj skutočnosť, kedy si spoločnosť cloudové služby prenajíma v porovnaní s modelom, kedy si ich spravuje sama.

Ďalšou výhodou cloudových služieb je možnosť skladovať veľké množstvo údajov na jednom mieste a umožniť prístup k nim a prácu s nimi väčšiemu počtu ľudí, prípadne vyšpecifikovaným jednotlivcom a skupinám.
Nevýhodu môže v praxi predstavovať najmä skutočnosť, že rôzne citlivé osobné a firemné informácie, údaje a dokumenty, sú uložené na cudzom hardvéri a niekedy aj na mieste, kam sa nikdy nedostanete a o ktorom ste možno nikdy nepočuli. To sa týka verejných alebo hybridných cloudov.
Narastajúcou hrozbou sú v súčasnosti aj potenciálne kybernetické útoky, ktorých cieľom je najmä krádež citlivých dát a informácií s cieľom ich zneužitia rôznymi spôsobmi voči jednotlivcom aj spoločnostiam.
Záver
Cloud predstavuje moderný spôsob ukladania a spracovávania dát cez internet, ktorý prináša firmám aj súkromným osobám množstvo rôznych výhod, ako je:
dostupnosť uložených a spravovaných údajov, obsahu a informácií,
flexibilita práce s uloženými a zdieľanými dátami,
rýchly prístup, možnosť zdieľania dát a spolupráce na veľké vzdialenosti,
produktivita a efektivita práce a pracovných postupov a procesov,
možnosť uloženia veľkého objemu dát na jednom mieste,
úspora nákladov.
Cloud umožňuje používateľom pristupovať k uloženým súborom na vlastných alebo externých dátových centrách z akéhokoľvek zariadenia s internetovým pripojením.

Vďaka tomu sa cloud výrazne zjednodušuje mnohé korporátne procesy a podporuje spoluprácu na diaľku. Cloud sa v súčasnosti zaraďuje medzi stálice digitálneho sveta a jeho význam bude v budúcnosti zrejme narastať spolu so zvyšujúcimi sa technologickými nárokmi v rôznych oblastiach.

Príloha 14 – Článok: Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady

Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady

Počítačová bezpečnosť a ochrana dát patria medzi základné oblasti, ktorým by mal rozumieť každý, kto pracuje s informáciami v online prostredí. Zameriava na ochranu dát a informácií pred neoprávneným prístupom, stratou či zneužitím. Kľúčové princípy, ako dôvernosť, integrita a dostupnosť údajov, tvoria základ tzv. bezpečnostnej triády, ktorá pomáha predchádzať kybernetickým hrozbám a chrániť citlivé informácie. V tomto článku sa pozrieme na to, čo tieto princípy znamenajú v praxi a ako ich efektívne uplatniť.

Základné princípy ochrany dát a informácií

Kybernetická bezpečnosť sa zaoberá ochranou údajov a informácií, ktoré sa primárne nachádzajú vo virtuálnom priestore. V praxi ide o dáta a informácie, ktoré sú uložené napríklad na rôznych vzdialených alebo firemných serveroch, počítačoch, datacentrách, internete alebo v mobilných zariadeniach.

Bezpečnostnú triádu v oblasti počítačovej bezpečnosti a ochrany dát tvoria tri kľúčové princípy, ktoré by mal poznať každý – nielen IT profesionál, ale aj bežný používateľ:

Dôvernosť

Pri každom spracovávaní akýchkoľvek údajov a informácií by ste vždy mali dodržiavať princíp dôvernosti. Toto pravidlo hovorí o tom, že každý údaj a informácia, s ktorou prídeme do kontaktu, by mali byť poskytnuté, zdieľané a šírené len s na to určenými a oprávnenými osobami. Každá dôverná informácia v sebe nesie potenciálne riziko zneužitia v osobnom a/alebo pracovnom živote a preto je kľúčové chrániť tieto dáta a informácie pred tými, ktorí by ich mohli zneužiť.

Za dôverné informácie sa označujú akékoľvek neverejné informácie, ktorých zverejnenie alebo poskytnutie by mohlo poškodiť jednotlivca a/alebo organizáciu.

Integrita

Integrita dát a informácií reprezentuje koncept úplnosti a správnosti údajov a informácií. Pri zabezpečovaní integrity dát sa v praxi aplikujú opatrenia, ktorých cieľom je zaistiť, aby boli tieto informácie neboli modifikované, zneužité alebo vymazané počas celého svojho životného cyklu.

Integrita dát je presnosť, úplnosť, konzistentnosť a spoľahlivosť údajov od ich vzniku až po ich zánik.

Dostupnosť

Dostupnosť konzistentných údajov a informácií znamená, že sú oprávneným osobám k dispozícii kompletné a vždy vtedy, keď ich potrebujú. Zároveň to indikuje, že tieto informácie sú takto chránené voči zneužitiu neoprávnenými osobami a/alebo subjektmi.

Uvedené tri princípy tvoria základ každej bezpečnostnej stratégie. Ak je v praxi porušený aj len jeden z týchto princípov, tak už systém ochrany dát štandardne nie je považovaný za bezpečný. Všetky tri oblasti sú navzájom úzko prepojené a jedna podporuje druhú.

Aj v rámci kybernetickej bezpečnosti platia všeobecné zásady ochrany osobných údajov podľa zákona č. 18/2018 o ochrane osobných údajov, ako sú napríklad:
Zákonnosť spracovania osobných údajov.
Obmedzenie účelu, za ktorým sa údaje spracovávajú.
Minimalizácia a presnosť spracovávaných údajov.
Obmedzenie doby archivácie spracovávaných údajov.
Obmedzenia v oblasti poskytovania a šírenia spracovávaných údajov.
Princípy, práva a povinnosti v súlade s platnou a účinnou slovenskou aj európskou legislatívou v oblasti ochrany osobných údajov.
Praktická aplikácia základných princípov ochrany dát
Počítačová bezpečnosť a ochrana dát by mali byť každodennou súčasťou firemných procesov, nielen teoretickým konceptom. Dodržiavanie princípov bezpečnostnej triády v praxi možete dosiahnuť aj nasledujúcimi praktickými opatreniami.
Dôvernosť v praxi
Hlavným cieľom tohto princípu je zabezpečiť, aby boli dáta a informácie dostupné len oprávneným osobám. Dôvernosť je kľúčovým aspektom najmä pri údajoch, ktoré sú označované ako osobné, bankové, zdravotné, strategické, firemné a podobné informácie.
Zaistiť bezpečnosť dát a informácií môžete viacerými spôsobmi:
Šifrovaním dát.
Udelením prístupových práv.
Viacfaktorovou autentifikáciou.
Autentifikáciou pomocou biometrických údajov.
Segregáciou citlivých údajov.
Obmedzením fyzického prístupu.
Integrita v praxi
Základným účelom princípu integrity je zabezpečiť, aby údaje ostali po celý čas svojej existencie kompletné, presné a nezmenené.
Zaistiť bezpečnosť dát a informácií môžete napríklad:
Digitálnym a elektronickým podpisom.
Revíznymi protokolmi.
Automatizovanou kontrolou zmien súborov.
Dostupnosť v praxi
Základným cieľom tohto ochranného princípu je zaistiť, že oprávnené osoby majú vždy dostupné údaje, ktoré potrebujú.
Zaistiť bezpečnosť dát a informácií môžete:
Pravidelnou kontrolou a zálohovaním dát a informácií.
Ochranou pred DDoS a ransonware útokmi.
Použitím redundantných systémov a serverov.
Použitím cloudu.
Použitím nezávislých napájacích zdrojov.
Monitoringom dostupnosti.
Zhrnutie na záver
Triáda bezpečnosti je základom každej bezpečnostnej politiky. Každé IT opatrenie navrhnuté na ochranu dát a informácií by tak malo zahŕňať všetky tri vyššie uvedené bezpečnostné princípy a tieto princípy by mali byť nastavené vo vzájomnej rovnováhe. Príliš silná dôvernosť môže znížiť dostupnosť dát a naopak. Pri analýze incidentov je následne dôležité definovať, ktorá časť triády bola zasiahnutá a následne prijať potrebné opatrenia na jej obnovenie alebo posilnenie.

Príloha 15 – Rozhovor s Ing. Michalom Papučíkom

„Moje meno je Michal Papučík, na projekte INNOSOC participujem ako architekt informačných systémov, analytik a vedecký výskumný pracovník. Projekt INNOSOC je z high level pohľadu aplikovaný výskum v oblasti kybernetickej bezpečnosti. Je to odpoveďou na dnešné nazvem to dopyty v oblasti kybernetickej bezpečnosti a to je moderné a bezpečné služby SASové cloudové služby a priniesť dostatok znalostí alebo expertov v oblasti kybernetickej bezpečnosti. Pôvodne sme chceli vytvoriť názov, ktorý by sa skladal štandardne z nejakých skratiek začiatočných písmen ale nakoniec sme dospeli k názoru že je to naše nové inovatívne riešenia nejakého Security Operation Centra, tak sme sa rozhodli že to INNO predstavuje ako inovatívnosť a SOC ako Security Operation Center, čiže dokopy skrátené INNOSOC. Hlavným cieľom projektu INNOSOC ako výskumného projektu v oblasti kybernetickej bezpečnosti je priniesť nejaké otvorené open source riešenie takým subjektom, ktoré si nemôžu dovoliť štandardné vysoko nákladové bezpečnostné riešenia, ktoré sa zaoberajú kybernetickou bezpečnosťou. Snažíme sa priniesť také riešeni,e ktoré si tie subjekty dokážu buď zajednať formou služby sa svojej služby alebo potom formou nejakého onpremise riešenia, ktoré je postavené na nejakej kontajnerizácii a nejakému jednoduchšiemu postaveniu u nich doma v systéme.
Projekt reaguje najmä na najväčšiu potrebu v rámci kybernetickej bezpečnosti a to je zabezpečiť naše informačné systémy. Nie sme na tom úplne dobre, čo sa týka Slovenskej republiky, naše IT systémy majú nespočetné množstvá problémov. Najväčšie nedostatky u nás sú okrem samotného zabezpečenia, že sú tie tieto bezpečnostné systémy veľmi nákladné a druhý faktor veľmi problémový je, že máme málo expertov, ktorí by dokázali tieto systémy obsluhovať alebo nejako pracovať v oblasti kybernetickej bezpečnosti. Naše riešenie vlastne zabezpečí to že si ho budú môcť dopriať alebo zabezpečiť také organizácie ktoré nám nemajú financie na tie drahé riešenia a zároveň vďaka umelej inteligencii alebo nejakému machine learningu dokážeme tak povediac odbremeniť tie náklady alebo tú potrebu tých expertov a nebude ich potrebné tak veľa.
Úplne najzakladanejší prínos za mňa pre to čo prinesieme z tohto projektu je že prinesieme návrh alebo nejaké riešenie open sourcové riešenie pre subjekty, ktoré si ho budú vedieť buď začať používať ako SASovú službu alebo si ho u seba onpremise spojazdniť. Ale pre mňa akože ďalšie ciele sú hlavne veľká spolupráca s univerzitnou sférou. To je prepojenie nazvem to firmy a univerzity a vytvoriť tak nejaký funkčný tím, ktorý dokáže nejaké myšlienky zaujímavé podnety pretaviť do nejakého hotového riešenia. A zároveň za mňa ako aj za univerzitu je to určite zvýšenie kompetentnosti týchto ľudí, ktorí na tom projekte participujú lebo každý sa naučí niečo nové a posunie sa ďalej v oblasti kybernetickej bezpečnosti.
Mňa na tomto projekte najviac bavia spoločné mítingy alebo nazval by som to skôr brainstormingy, kde sa všetci spolu dohadujeme. Nie je to vždycky úplne že najmilšie a najkrajšie ale vždycky si povieme, čo sú dôležité faktory, ako ich vieme dosiahnuť, hľadáme spoločný nápady, konsenzus. Možno táto synergia medzi týmito dvoma tímami z univerzity z výskumného prostredia a nášho z toho firemného alebo nazvem to z toho, čo rieši tú praktickú stránku vecí je častokrát vymyslenie niečoho úplne nového alebo nového prístupu. To ma naozaj teší, že nerobíme niečo bežné, ale naozaj sa ide do niečoho nového čo sa snažíme tak skĺbiť dokopy týchto oboch svetov.
Na projekte INNOSOC sme sa stretli naozaj s veľkým množstvom technológií. Keď si odmyslím tie bezpečnostné a kyberbezpečnostné technológie, ako sú hardvér a softvér v oblasti bezpečnosti, tak veľmi často sme sa stretli napríklad s bežným

hardvérom od softvéru, hardvéru v infraštruktúre, sieťové prvky okrem firewallov, štandardné routere, switche a tak ďalej, koncové stanice, množstvo iných zariadení ako sú aj tablety, mobily, čiže štandardne s tým prichádzame do styku. Ale medzitým sme si vyskúšali mnoho rôznych databáz napríklad alebo prezentačných vrstiev, nejakých programov, ktoré už reprezentujú nejaké logy, nejaké záznamy, nejaké anomálie. A zároveň dosť sme sa tak povediac vyhrali aj s nejakými modelmi umelej inteligencie alebo machine learningu prípadne inak nazvaného strojového učenia.
Úloha našej spoločnosti BRAIN:IT na projekte bola spočiatku rozdelená hlavne na základe našich kompetencií. Už v úvode sme si povedali že dobre, my máme veľkú výhodu alebo sme silní práve v tej oblasti, že vieme zobrať nejaké vyskúmané informácie ktoré niekto predpracuje, čo je v tomto prípade univerzita, a my z nich prepracujeme nejaký produkt alebo projekt alebo pôjdeme s ním ďalej a urobíme návrh ktorý je použiteľný v praxi. Čiže to sú naše silné stránky. Preto sme sa aj rozhodli že naše pracovné balíky sú najmä konfigurácia a inštalácia týchto podmodulov alebo modulov. Zároveň to bol návrh architektúry jej vytvorenie a ako tretie sme si zobrali na starosti alebo sme garantmi osvetovej alebo marketingovej činnosti dostať to povedomie medzi ľudí o tomto projekte a o tejto kybernetickej bezpečnosti a týchto oblastiach okolo toho.
Musím aj samozrejme podotknúť že na všetkom sme spolupracovali spoločne. To bola aj idea keď sme do tohto projektu išli, tam bola jasná vízia a dohoda, že určite na každom work packagei pracujeme spolu. Už len kvôli tomu, aby sme prehĺbili tú spoluprácu, nech je intenzívna a nech sa všetci naučia z tej oblasti v ktorej nie sú zvyknutí pracovať. To znamená škola sa naučí niečo od nás a my niečo zo školy.
Prepájať akademickú a biznis sféru je podľa mňa úplne výhodné práve takýmito projektami ktoré sú výskumné, skĺbené spolu s niečím ktoré už presahujú do toho, že sa vytvára nejaký produkt. Vďaka tomu my sme si napríklad vytvorili také partnerstvo ktoré už ďaleko presahuje hranice projektu, už spolupracujeme na iných projektoch. Určite aj po ukončení budeme spolupracovať na úplne iných oblastiach ako len kybernetickej bezpečnosti. A už teraz napríklad spolu sme napísali ďalší projekt, ktorý je pokračovanie INNOSOC-u a mal by ho dostať na ďalší level kdesi ďalej v tej našej vízii, kde ho chceme dostať.
Na projekte INNOSOC využívame množstvo medzinárodných štandardov. Úplne ako prvý spomeniem Prince 2, to je metodika riadenia projektov, ktorej sa dodržujeme, lebo na Fakulte riadenia informatiky je to zaužívaný proces alebo framework. Rovnako u nás v spoločnosti BRAIN:IT ho používame na všetky projekty a veľmi nám pomáha v dodávke týchto projektov. Zároveň ITIL V používame kvôli nastaveniu nejakých servisných parametrov, servisných službám a v oblasti správy týchto služieb ktoré plánujeme v budúcnosti budovať.
Čo sa týka architektúry, tak tam sme si povedali že budeme využívať nejaký architektonický rámec určený TOGAFom. Najčastejšie čo sa týka nejakej reprezentácie grafickej využívame Archimate 1 alebo UML verzia 2. Niekedy aj BPML, ale nie je to úplne až tak striktne dané, v tomto prípade drvivá väčšina je Archimate a UMLO verzia 2.
Čo sa týka štandardov našej spoločnosti, tak ako prvý určite musím vymenovať ISO 27001, čo je vlastne informačná bezpečnosť ktorá priamo s tým súvisí. Takisto 9001 dodržiavame, 22 301 a mnohé iné ako aj 20 000 o riadení služieb.“

Príloha 16 – Rozhovor s prof. Ing. Pavlom Segečom, PhD.

Moje meno je Pavel Segeč. Pracujem ako vedúci Katedry informačných sietí na Fakulte riadenia a informatiky. V projekte INNOSOC som kľúčovým riešiteľom projektu. Kybernetická bezpečnosť je pre mňa v súčasnosti kľúčovou témou, pretože žijeme v dobe, keď je všetko navzájom poprepájané a sme v online komunite. Siete sa stávajú digitálnymi diaľnicami, ktoré umožňujú a podporujú naše správanie, biznis a ďalšie aspekty nášho života.

Za mňa je kybernetická bezpečnosť dôležitá pre malé firmy z viacerých dôvodov. Tieto základné dôvody môžu byť buď zákonné náležitosti, ktoré sú dané novou novelizáciou zákona o kybernetickej bezpečnosti. Druhým aspektom je, že práve v dobe, keď sme všetci prepojení, by malo byť bezpečné správanie pre každého základom, nakoľko každý z nás má vlastné kritické aktíva, ktoré považuje za citlivé a ktoré treba chrániť.

Fakulta riadenia a informatiky je v projekte INNOSOC hlavným žiadateľom projektu a zároveň kľúčovým vedeckovýskumným partnerom. V rámci projektu INNOSOC poskytujeme svoje výskumné kapacity a zároveň aj našu privátnu cloudovú infraštruktúru ako koncept, na ktorom je možné realizovať pilotné nasadenia technológií, ktoré sú v projekte vyvíjané a skúšané.

Medzi najčastejšie hrozby v súčasnosti, ak to podoprieme štatistickými údajmi, patria rôzne phishingové kampane. Samozrejme, veľmi obľúbenou témou je ransomvér (ransomware) a kryptomvér, ktorý je momentálne veľmi aktívny. Okrem toho však považujem za veľmi dôležitú tému takzvaných APT (Advanced Persistent Threats). Ide o pokročilé útoky, pri ktorých sú útočníci dlhodobo umiestnení v sieti obete a vykonávajú špionáž a monitorovanie. Mnohokrát ide o stovky dní, počas ktorých daná spoločnosť netuší, že má vo svojej sieti útočníka.

Security Operations Center (SOC) nie je len jedna technológia, pretože SOC centrá stoja na troch pilieroch: ľudia, procesy a technológie. Nás, samozrejme, ako technologického partnera projektu, zaujímajú práve technológie. Úlohou SOC centier je v súčasnosti pomáhať detekovať a najmä reagovať na odhalené útoky alebo útočníkov, ktorí sa v sieti nachádzajú.

Téma SOC je dôležitá aj z toho dôvodu, že práve novelizáciou a sprísnením kybernetického zákona a jeho vyhlášky, ktorá je už momentálne dostupná, sa rozširuje množstvo firiem, ktoré sa musia aktívne správať a chrániť pred rôznymi typmi hrozieb a musia reportovať detekované hrozby, ktoré boli odhalené. Práve hlavným cieľom SOC centier je pomôcť firmám detekovať a reagovať na hrozby, ktoré sa v ich sieťach vyskytli.

Vďaka smernici NIS2, ktorá bola transponovaná do slovenskej legislatívy, sa sprísnili požiadavky na zvýšenie úrovne bezpečnosti a riadenia bezpečnosti v spoločnostiach. Zároveň sa sprísnili aj aspekty spojené s reportovaním útokov. Práve reportovaniu útokov a ich odhaľovaniu by mali pomôcť SOC centrá, čo je vlastne téma, ktorú riešime v projekte INNOSOC.

SOC centrá technologicky fungujú na princípe telemetrického zberu veľkého množstva údajov. Tieto údaje sú následne ukladané do databáz a obohacované o rôzne doplnkové údaje za účelom jednoduchšej detekcie a odhalenia anomálneho správania.

Stále však hovoríme o obrovskom množstve zbieraných údajov, a preto je v súčasnosti jedným z trendov, ktoré sa implementujú do SOC, podpora umelej inteligencie a strojového učenia. Práve zavedenie týchto metód strojového učenia do riešení SOC je jedným z aspektov, ktoré v spolupráci s BRAIN:IT riešime v rámci nášho vývoja v projekte INNOSOC.

Príloha 17 - Článok o rozhovore s odborníkmi Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakonm, PhD

V rámci prác na výskumnom projekte INNOSOC bol realizovaný rozhovor s jeho kľúčovými odborníkmi – Dominikou Toman a Martinom Mičiakom z Fakulty riadenia a informatiky Žilinskej univerzity v Žiline (FRI UNIZA).
Rozhovor prináša hlbší pohľad na to, ako prebieha prepojenie akademického výskumu s reálnou praxou v oblasti kybernetickej bezpečnosti.
Čo je cieľom projektu INNOSOC?
Projekt sa zameriava na prepájanie výskumu a inovácií v oblasti SecurityOperationCenters (SOC). Jeho hlavným zámerom je:
Vytvoriť technologické riešenia a návrhy pre organizácie, ktoré si chcú zabezpečiť svoju kybernetickú bezpečnosť.
Poskytnúť alternatívu k drahým komerčným riešeniam využitím a integráciou vhodných open-source komponentov.
Priniesť využiteľné výstupy pre verejnú správu, podniky a odbornú komunitu.
Úloha manažmentu vo výskume
Hoci je téma projektu vyslovene technická, Dominika Toman a Martin Mičiak zastupujú Katedru manažérskych teórií. Ich rola spočíva predovšetkým v riadení a koordinácii celého projektu.
V rozhovore zdôraznili, že projekt je pre nich vynikajúcou príležitosťou aplikovať poznatky z projektového manažmentu priamo v praxi. Skúsenosti z riadenia technických odborníkov a spolupráce s biznis partnerom (spoločnosť BRAIN:IT) následne prenášajú aj do výučby a prednášok pre svojich študentov.
Výzvy a riadenie rizík
Práca na takomto komplexnom projekte prináša viaceré výzvy, ktoré boli predmetom diskusie:
Koordinácia partnerov: Zladenie akademického prostredia s biznis sférou a riešenie komunikačných šumov.
Časový harmonogram: Výzvou bolo napríklad zladenie povinných dovoleniek na univerzite s plánovanými stretnutiami projektového tímu.
Vedecká činnosť: Príprava indexovaných vedeckých výstupov a publikácií je zdĺhavý proces, ktorý si vyžaduje plánovanie s veľkým predstihom kvôli recenzným konaniam.
Prínos pre prax a odbornú komunitu
Najvýznamnejším výstupom projektu je podľa odborníkov tzv. „proof of concept“ – overenie, že navrhnutá architektúra postavená na open-source nástrojoch je reálne aplikovateľná a udržateľná.
Pre malé podniky a organizácie verejnej správy to znamená možnosť zvýšiť svoju ochranu pred kybernetickými hrozbami aj bez potreby obrovských finančných investícií do licencií alebo budovania vlastnej expertízy „od nuly“.

Článok je výstup z projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia.“

Kód projektu – 09I05-03-V02-00010.

Príloha 18 - Článok o rozhovore o projekte INNOSOC: Kybernetická bezpečnosť a rozširovanie obzorov s Dominikou Toman

Prinášame vám pohľad do zákulisia projektu INNOSOC prostredníctvom rozhovoru s Ing. Dominikou Toman, PhD., odbornou asistentkou na Katedre manažérskych teórií Fakulty riadenia a informatiky Žilinskej univerzity v Žiline. V projekte zastáva kľúčovú úlohu pri podpore projektového riadenia a koordinácii ľudí.

Význam projektu pre verejnosť a odbornú prax

Podľa Dominiky Toman je hlavným prínosom projektu pre širokú i odbornú verejnosť najmä rozširovanie obzorov v oblasti kybernetickej bezpečnosti. Projekt sa zameriava na odovzdávanie základných informácií o riešeniach, ktoré môžu v tejto dôležitej sfére pomôcť.

Pre odbornú prax sú kľúčové najmä tieto aktivity:

Intenzívna publikačná činnosť a prezentovanie informácií na odborných konferenciách.

Tvorba rešerší o najvhodnejších riešeniach pre podporu kybernetickej bezpečnosti.

Príprava podkladov pre školenia zamestnancov, ktoré organizáciám pomôžu efektívne ovládať nové bezpečnostné riešenia.

Osobný rozvoj a spolupráca

Účasť na projekte priniesla cenné skúsenosti aj samotným riešiteľom. Dominika Toman vyzdvihla, že vďaka INNOSOC-u nadobudla množstvo nových informácií a výrazne si zdokonalila svoje zručnosti v oblasti riadenia a koordinácie.

Projekt zároveň vytvára priestor na intenzívnu komunikáciu s partnermi, a to nielen v rámci akademickej pôdy, ale aj priamo s odborníkmi z praxe, čo prispieva k vytváraniu kvalitných a využiteľných výstupov.

Článok je výstup z projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia.“

Kód projektu – 09I05-03-V02-00010.

Príloha 19 - Článok o rozhovore o projekte INNOSOC: O vedeckom výskume a kybernetickej bezpečnosti s Martinom Mičiakom

Pokračujeme v sérii rozhovorov o projekte INNOSOC, tentokrát s Ing. Martinom Mičiakom, PhD., z Katedry manažérskych teórií Fakulty riadenia a informatiky Žilinskej univerzity v Žiline. V projekte pôsobí ako výskumný pracovník a zároveň je súčasťou tímu pre podporu projektového riadenia.

Kybernetická bezpečnosť a význam kvalitnej vedy

Hlavnou témou projektu INNOSOC je kybernetická bezpečnosť a hľadanie spôsobov, ako ju v organizáciách posilniť. Martin Mičiak zdôrazňuje, že projekt sa zameriava najmä na open-source riešenia, ktoré umožňujú zvýšiť ochranu aj pri nižších celkových nákladoch.

Pre úspech projektu je podľa neho kľúčová kvalita vedeckých výstupov:

Publikovanie v renomovaných vydavateľstvách a indexovaných časopisoch či databázach.

Zvyšovanie relevantnosti a povedomia o projekte v očiach odbornej komunity i širokej verejnosti.

Dôraz na praktickú využiteľnosť výsledkov pre prax.

Výzva v podobe „výskumnej medzery“

V rozhovore Martin Mičiak priblížil aj náročnosť vedeckej práce. Za najťažšiu časť považuje samotný výskum – schopnosť správne zmapovať danú oblasť a identifikovať tzv. research gap (výskumnú medzeru). Cieľom je, aby každý príspevok na konferenciu alebo článok prinášal niečo nové a zaujímavé, čo posúva tému kybernetickej bezpečnosti vpred.

Prepojenie manažmentu, informatiky a biznisu

Projekt INNOSOC je unikátny svojou kombináciou akademického a biznis prostredia. Na pôde fakulty ide o dôležitú spoluprácu dvoch pracovísk:

Katedry manažérskych teórií

Katedry informačných sietí

Táto kooperácia umožnila Martinovi Mičiakovi hlbšie prepojiť manažérsku a informatickú oblasť, rozšíriť si obzory v kybernetickej bezpečnosti a získať ďalšie cenné praktické skúsenosti v oblasti riadenia projektov

Článok je výstup z projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia.“

Kód projektu – 09I05-03-V02-00010.

Príloha 20 – Článok o prof. Ing. Milanom Kubinom, PhD. o projekte INNOSOC

V rámci odborného dialógu nám prof. Ing. Milanom Kubinom, PhD., predstavil strategické smerovanie projektu INNOSOC, ktorý primárne reaguje na narastajúce riziká zneužívania systémových zraniteľností v digitálnom prostredí.
Projekt sa zameriava na vývoj inovatívnych nástrojov pre SOC (Security Operations Center) a správu IP sietí, s osobitným dôrazom na zvyšovanie kybernetickej reziliencie subjektov s limitovanými rozpočtovými možnosťami, ako sú malé firmy, orgány verejnej správy a školské zariadenia.

V rozhovore odborník prezradil, v akej fáze sa vývoj nachádza, aj to prečo je synergia medzi akademickou sférou a aplikačnou praxou realizovanou so spoločnosťou BRAIN:IT taká dôležitá.

Článok je výstup z projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia.“

Kód projektu – 09I05-03-V02-00010.

Príloha 21 – Popularizačný článok na tému Prepojenie AI a kybernetickej bezpečnosti v praxi

Kybernetické útoky sú čoraz častejšie a zároveň sofistikovanejšie. Hoci umelá inteligencia dokáže výrazne zefektívniť mnohé procesy, odborníci upozorňujú, že pri ochrane pred kybernetickými hrozbami by nemala fungovať ako jediné riešenie. Kombinácia a spolupráca AI a človeka dokáže do praxe vniesť väčšiu rovnováhu a vyťažiť maximum zo silných stránok oboch týchto hráčov. V článku sa bližšie pozrieme na prepojenie umelej inteligencie (AI) a ľudského faktora v oblasti kybernetickej bezpečnosti.

Využitie AI pri detekcii a prevencii kybernetických útokov

Využitie AI v rôznych oblastiach môže priniesť zvýšenú efektivitu, produktivitu, úsporu času a peňazí. Umelá inteligencia dokáže skvelým spôsobom zastúpiť mnohé pracovné výkony, ktoré sú pre človeka namáhavé a vyčerpávajúce, a okrem toho je schopná vykonávať tieto úlohy nepretržite a bez potreby oddychu.

V mnohých situáciách tak dokáže AI eliminovať riziko ľudského pochybenia, ktoré je často výsledkom únavy a nepozornosti. Jedným dychom však treba dodať, že ani umelá inteligencia nie je neomylná a môže prezentovať nepravdy ako fakty a správne informácie. K týmto situáciám môže dôjsť napríklad pri zle nastavenom algoritme alebo v prípade, že bola AI trénovaná na nesprávnych dátach.

Úloha AI v kybernetickej bezpečnosti

Detekcia kybernetických hrozieb v reálnom čase

Tradičné systémy často reagujú až vtedy, keď útočníci preniknú do siete alebo systému. AI však dokáže analyzovať správanie používateľov a zariadení v reálnom čase, rozpoznávať nezvyčajné vzorce správania a okamžite tak upozorniť na rizikové aktivity.

Predpoveď kybernetických útokov

Vďaka veľkému množstvu dát, z ktorých AI čerpá svoje poznatky, dokáže v reálnom čase efektívne rozpoznávať vzory, ktoré v minulosti predchádzali útokom, prípadne identifikovať neobvyklé vzorce správania a odhaliť tieto anomálie.

Automatizácia reakcií

AI dokáže automaticky izolovať infikované zariadenia, blokovať komunikáciu s podozrivými servermi alebo spustiť postupy incident response ešte pred zásahom človeka.

Výsledkom je rýchlejšia reakcia, včasné odhalenie reálneho kybernetického útoku a tým aj minimalizácia prípadných škôd.

AI ako dvojsečná zbraň

Hoci je AI účinným a efektívnym nástrojom kybernetickej bezpečnosti, má aj svoje limity. Môže sa stať aj silnou zbraňou v rukách útočníkov.

Ako AI používajú kybernetickí útočníci?

Automatizované útoky: AI možno využívať na automatizovanú ochranu, ale aj na generovanie automatických phishingových e-mailov a vedenie iných útokov vo veľkom rozsahu.

Deepfake a sociálne inžinierstvo novej generácie: Veľkú hrozbu v súčasnosti predstavuje fenomén tzv. deepfake audií a videí, ktoré umožňujú psychologickú manipuláciu ľudí, akú sme ešte donedávna poznali len z najodvážnejších sci-fi filmov. Sfalšované identity, fotografie, účty či rôzne citlivé osobné a obchodné informácie sú pre laika bez špeciálnych technológií často nerozoznateľné a dokážu zdevastovať životy aj kariéry ľudí.

Zneužitie generatívnych modelov: Generatívna AI môže byť použitá aj na tvorbu škodlivého kódu, automatizáciu škodlivých kampaní či obchádzanie detekčných mechanizmov.

Prepojenie AI s kybernetickou bezpečnosťou tak spočíva vo vyváženej spolupráci umelej inteligencie a ľudského faktora.

Výhody a riziká AI v oblasti kybernetickej bezpečnosti

Ak využívate umelú inteligenciu v oblasti kybernetickej bezpečnosti, jej najväčšou výhodou je schopnosť pracovať s obrovským množstvom dát v reálnom čase. AI pomáha rýchlejšie vyhodnocovať riziká, podporuje rozhodovanie bezpečnostných tímov a uľahčuje strategické plánovanie tam, kde by manuálna analýza zlyhala.

Zároveň však platí, že AI systémy musia byť pod kontrolou. Aby ste minimalizovali chyby, potrebné rozumieť tomu, ako a prečo AI reaguje určitým spôsobom. Transparentnosť, auditovateľnosť rozhodnutí a pravidelné preverovanie výstupov sú dôležité najmä v prostredí, kde ide o citlivé údaje. Rovnako podstatné je priebežné trénovanie a aktualizácia AI modelov, aby pracovali s aktuálnymi a overenými dátami.

Umelá inteligencia nemá nahradiť prácu bezpečnostných analytikov, ale ju posilniť. Najlepšie výsledky dosiahnete vtedy, keď technológie podporujú ľudský úsudok. S rastúcim využívaním AI preto prirodzene prichádza aj potreba riešiť etické otázky, zodpovedné nastavenie procesov a jasné pravidlá ochrany pred zneužitím údajov.

Článok je výstup z projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia.“ Kód projektu – 09I05-03-V02-00010.

Príloha 22 – Popularizačný článok na tému Kybernetické útoky: Ako sa menia a prečo predstavujú čoraz väčšie riziko

Kybernetické útoky už dnes nie sú len dielom technicky zdatných osamelých jednotlivcov. Za čoraz sofistikovanejšími kybernetickými hrozbami stoja komplexné organizované skupiny a profesionálni hackeri, ktorí využívajú najmodernejšie technológie, rôzne automatizačné nástroje, techniky či umelú inteligenciu. Spoznajte hlavné dôvody, prečo sa kybernetické útoky stávajú čoraz sofistikovanejšími.

Hlavné dôvody sofistikovanejších kybernetických útokov

Kybernetické útoky sú v súčasnosti nielen čoraz častejším fenoménom, ktorý sa nevyhýba jednotlivcom, firmám ani rôznym obchodným či štátnym organizáciám, ale sú aj čoraz sofistikovanejšie. Všade tam, kde existujú citlivé údaje, potenciálne hrozí riziko ich zneužitia. Mnohé údaje sa dnes nachádzajú aj v online priestore, ktorý sa preto stáva čoraz častejším terčom záujmu profesionálov snažiacich sa k týmto údajom dostať a zneužiť ich.

Hrozby internetu sú tak svojím spôsobom prirodzeným vyústením nášho technologického vývoja. Medzi hlavné príčiny, pre ktoré sú kybernetické útoky čoraz nebezpečnejšie, patria:

Organizované skupiny a organizovaná spolupráca

Jedným z hlavných dôvodov je organizovaná povaha kybernetických útokov. Útoky vykonávajú skúsení profesionálni hackeri, ktorí sú dobre organizovaní, vybavení najmodernejšími technológiami a disponujú najnovšími technickými a IT znalosťami.

Pokročilé techniky a trendy

Mnohí hackeri a organizované skupiny kybernetických útočníkov zneužívajú pokročilé metódy, techniky a trendy, ktoré zasahujú nielen do oblasti informačných technológií, ale aj sociálneho inžinierstva. Útočníci pritom využívajú slabiny ľudskej psychiky a rôzne manipulatívne techniky.

Pôsobnosť v online priestore

Ako už bolo naznačené vyššie, jedným z dôvodov rozšírenia kybernetických útokov je aj skutočnosť, že v online priestore trávime veľa času, čím sa rozširuje okruh potenciálnych cieľov kybernetických útokov.

Využívanie umelej inteligencie (AI)

Umelá inteligencia výrazne mení spôsob, akým vznikajú kybernetické útoky. Útočníci ju čoraz častejšie využívajú na automatizáciu útokov, vytváranie presvedčivých phishingových e-mailov či falšovanie digitálneho obsahu, účtov a identít. Vďaka AI sú tieto útoky rýchlejšie, cielenejšie a pre bežných používateľov ťažšie rozpoznateľné.

Práve preto je dôležité, aby jednotlivci aj firmy držali krok s týmto vývojom. Základom je priebežné vzdelávanie v oblasti kybernetickej bezpečnosti a dôsledné uplatňovanie ochranných opatrení, ktoré pomáhajú predchádzať zneužitiu dát a bezpečnostným incidentom.

Dopady kybernetických útokov na praktický život

Dopady čoraz častejších a sofistikovanejších kybernetických útokov na bežných ľudí, firmy a iné organizácie možno v praxi rozdeliť do troch základných skupín:

Organizácie aj jednotlivci čelia neustále rastúcemu počtu pokusov o prienik do ich súkromia a pracovného prostredia s cieľom zneužitia ich údajov.

V reakcii na tieto situácie vzniká naliehavá potreba komplexne riešiť ochranu citlivých údajov v reálnom čase. Ukazuje sa, že doterajšie ochranné mechanizmy rýchlo zastarávajú a je potrebné na nové hrozby reagovať promptne.

Logickým vyústením oboch predchádzajúcich faktorov sú zvýšené výdavky jednotlivcov aj firiem na bezpečnosť a ochranu pred kybernetickými hrozbami, ktoré sú čoraz častejšie asofistikovanejšie.

V praxi sa často ukazuje, že zastaraný antivírusový softvér alebo základné bezpečnostné opatrenia už na dnešné hrozby nestačia. Útočníci dokážu takéto ochrany obísť a získať prístup k citlivým údajom. Následkom býva zneužitie osobných alebo firemných dát na neoprávnené finančné operácie, administratívne komplikácie a riešenie dôsledkov, ktoré môžu viesť až ku komunikácii s úradmi či políciou. Okrem finančných strát ide často aj o stratu dôvery a narušenie bežného fungovania jednotlivcov či firiem.

Ochrana pred kybernetickými útokmi

Ochrana pred kybernetickými útokmi dnes nie je jednorazovým rozhodnutím, ale dlhodobým prístupom. Nestačí mať zapnutý antivírus alebo používať silné heslo. Dôležité je rozumieť tomu, kde sa vaše údaje nachádzajú, kto k nim má prístup a akým spôsobom sú chránené.

V praxi to znamená pravidelne si klásť jednoduché, no podstatné otázky:

Kde sú uložené moje osobné alebo firemné dáta?

Komu ich poskytujem a z akého dôvodu?

V akom rozsahu ich zdieľam a je to skutočne nevyhnutné?

Významnú úlohu zohráva aj priebežný dohľad nad systémami a dátami. Nepretržitý monitoring umožňuje včas zachytiť podozrivé správanie a reagovať skôr, než vzniknú reálne problémy. Pre firmy aj jednotlivcov tak predstavuje praktický spôsob, ako minimalizovať finančné straty, administratívne komplikácie a narušenie dôvery.

V konečnom dôsledku je práve kombinácia technických riešení a vedomej práce s údajmi tým, čo pomáha zvládať čoraz sofistikovanejšie kybernetické hrozby bez zbytočného rizika.

Článok je výstup z projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia.“ Kód projektu – 09I05-03-V02-00010.

Príloha 23 – Popularizačný článok na tému Automatizácia a hlboké strojové učenie v kybernetickej bezpečnosti

Automatizácia v kybernetickej bezpečnosti je odpoveďou na rastúci objem bezpečnostných udalostí, ktoré už nie je možné efektívne analyzovať manuálne. Organizácie preto čoraz častejšie využívajú automatizáciu a hlboké strojové učenie (deep learning), ktoré umožňujú detekciu hrozieb v reálnom čase a rýchlu reakciu na incidenty. V článku vysvetľujeme, ako funguje automatická detekcia hrozieb, aké má obmedzenia a prečo aj pri pokročilých technológiách zostáva ľudský zásah nenahraditeľný.

Prečo je automatizácia v kybernetickej bezpečnosti nevyhnutná?

Automatizácia v kybernetickej bezpečnosti je nevyhnutná najmä preto, že objem hrozieb a bezpečnostných dát neustále rastie. Vykonávanie manuálnej kontroly by bolo neefektívne a len veľmi ťažko zvládnuteľné.

Okrem toho je automatická detekcia kybernetických útokov dôležitá aj z viacerých ďalších dôvodov:

zložitejšie a rafinovanejšie kybernetické útoky,

limity manuálneho dohľadu v reálnom čase,

nižší počet falošných poplachov,

efektívnejšie využitie ľudských zdrojov.

Hlboké strojové učenie v bezpečnostnom kontexte

Hlboké strojové učenie (deep learning) je pokročilá forma strojového učenia. V oblasti kybernetickej bezpečnosti slúži na automatickú detekciu hrozieb a analýzu správania systémov, zariadení a používateľov. Vďaka využívaniu viacvrstvových neurónových sietí dokáže spracovať aj veľké objemy dát a identifikovať vzorce typické pre kybernetické útoky, phishing či malware.

Rozdiel medzi strojovým učením a hlbokým učením

Strojové učenie pracuje s vopred definovanými znakmi, ktoré do modelu pripravuje človek. Na druhej strane hlboké strojové učenie si tieto znaky dokáže odvodiť samo, a to automaticky priamo z dát.

Jednoducho povedané, deep learning zvláda komplexnejšie a menej zjavné vzorce správania. Táto vlastnosť je v kybernetickej bezpečnosti mimoriadne dôležitá, najmä pri detekcii nových alebo neznámych typov útokov.

Ako sa modely učia rozpoznávať bezpečnostné hrozby?

Modely hlbokého strojového učenia sa trénujú na veľkých množstvách historických bezpečnostných dát, ktoré obsahujú bežné aj škodlivé správanie. Počas tréningu sa neurónové siete učia rozlišovať medzi normálnou aktivitou a anomáliami, ktoré môžu predstavovať kybernetický útok.

Výhody automatizácie a deep learningu pri odhaľovaní kybernetických útokov

Medzi hlavné výhody AI v kybernetickej bezpečnosti patrí schopnosť včas odhaľovať rôzne typy útokov. V praxi tieto technológie fungujú tromi základnými spôsobmi:

1. Detekcia anomálií v reálnom čase

Ide o jeden z najdôležitejších benefitov automatizácie bezpečnosti. Modely využívajúce deep learning poznajú bežné správanie aplikácií či sietí, vďaka čomu dokážu pomerne jednoducho odhaliť aj tie najmenšie anomálie. Robia tak v reálnom čase, čím minimalizujú dopad útokov a zabezpečujú plynulú prevádzku.

2. Analýza správania používateľov a zariadení

Táto analýza má viacero funkcií. Slúži predovšetkým na sledovanie:

vzorcov prihlasovania,

práce so súbormi,

pohybu v sieti,

komunikácie medzi zariadeniami.

Ak sa v týchto oblastiach objavia odchýlky, ktoré môžu naznačovať prítomnosť malvéru, systém ich začne okamžite riešiť. Takýto prístup je bežný v mnohých oblastiach, vrátane riešení typu SIEM (Security Information and Event Management) alebo EDR (Endpoint Detection and Response).

3. Predikcia bezpečnostných incidentov

Dôležitú úlohu zohráva aj prediktívna analýza bezpečnosti. Jej cieľom je odhadnúť pravdepodobnosť budúcich incidentov na základe historických dát. Systémy vyhodnocujú trendy, opakujúce sa vzorce a slabé miesta infraštruktúry, čo im umožňuje identifikovať riziká ešte predtým, ako dôjde k samotnému útoku.

Automatizovaná reakcia na incidenty (SOAR) v praxi

SOAR predstavuje významnú súčasť modernej kybernetickej bezpečnosti, ktorá skracuje čas medzi detekciou hrozby a samotným zásahom. V kombinácii s

automatizáciou bezpečnosti, strojovým učením a nástrojmi typu SOAR je možné reagovať na útoky takmer okamžite. V praxi to výrazne znižuje rozsah škôd a obmedzuje šírenie útoku v rámci infraštruktúry.

Izolácia zariadení a obmedzenie prístupu – ak systém na základe analýzy správania vyhodnotí koncový bod ako rizikový, môže automaticky obmedziť jeho prístup k sieti alebo ho úplne odpojiť.

Automatizované bezpečnostné scenáre – definujú konkrétne postupy, ako reagovať na rôzne typy incidentov. V prípade vzniku hrozby systém automaticky spustí prednastavený postup.

Limity automatizácie a riziká deep learningu v bezpečnosti

Hoci má automatizácia bezpečnosti množstvo výhod, prináša so sebou aj určité limity a riziká. Patrí medzi ne napríklad nesprávne vyhodnotenie situácie a vznik falošných poplachov, ako aj závislosť od kvality tréningových dát. Ak sú dáta neúplné alebo skreslené, modely sa môžu učiť nesprávne vzorce správania.

Automatizácia nenahrádza človeka, ale mení jeho úlohu

Umelá inteligencia síce dokáže automaticky detegovať hrozby a reagovať na incidenty, no stále nedokáže plne pochopiť kontext a chýba jej strategické myslenie aj pocit zodpovednosti. Automatizácia preto preberá najmä rutinné a časovo náročné úlohy, no v súčasnosti nedokáže úplne nahradiť bezpečnostných analytikov. Tí sú nevyhnutní pri interpretácii výsledkov, vyšetrovaní zložitejších incidentov či nastavovaní bezpečnostnej stratégie.

Budúcnosť automatizácie v kybernetickej bezpečnosti

V nasledujúcich rokoch môžeme očakávať vyššiu presnosť a užšiu spoluprácu medzi technológiami a človekom. Vďaka automatizácii by mala byť detekcia hrozieb rýchlejšia a presnejšia, čo povedie k vyššej efektivite a produktivite práce. Samozrejmosťou by mal byť aj nižší počet falošných poplachov a väčší dôraz na kvalitu dát.

Výrazný posun povedie k tomu, že na umelú inteligenciu sa budeme môcť spoliehať ešte viac. Aj napriek tomu však nebude pôsobiť ako úplná náhrada ľudského faktora, ktorý zostane nevyhnutný aj v nasledujúcich rokoch.

Článok je výstup z projektu „Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia.“ Kód projektu – 09I05-03-V02-00010.

Príloha 24 – Rozhovor s Ing. Dominikou Toman, PhD. a Ing. Martinom Mičiakom, PhD.

Projekt INNOSOC prepája výskum, prax a inovácie v oblasti kybernetickej bezpečnosti a Security Operation Centier. Jeho cieľom je priniesť nové poznatky a použiteľné výstupy pre verejnú správu, podniky a odbornú komunitu. Dnes sa o projekte budeme rozprávať s Dominikou Toman a Martinom Mičiakom, ktorí patria

medzi kľúčových odborníkov zapojených do výskumu za partnera projektu, ktorým je Fakulta riadenia a informatiky Žilinskej univerzity v Žiline.

Ako by ste popísali projekt niekomu, kto o ňom počuje prvýkrát?

Projekt sa sústreďuje na vytvorenie technologického riešenia alebo návrhu pre organizácie, ktoré by si chceli zabezpečiť svoju bezpečnosť v rámci ich fungovania. Odlišuje sa tým, že je zameraný aj na organizácie, ktoré si nemôžu dovoliť drahé komerčné riešenia, a preto sa hľadala kombinácia vhodných komponentov z open source prostredia. Prináša to jedinečnú integráciu častí riešenia a pre nás to bolo zaujímavé aj kvôli kombinácii akademického prostredia s biznis partnerom – spoločnosťou BRAIN:IT. Ukazuje to verejnosti, že sa dá robiť naozaj úzko prepojená spolupráca medzi univerzitami a podnikmi.

Aké sú vaše roly a činnosť na projekte?

Z našej fakulty sú zapojené dve katedry: Katedra informačných sietí a my – Katedra manažérskych teórií. My zastrešujeme riadenie a koordináciu, čiže menej technického a viac manažérskeho. Je to pre nás príležitosť aplikovať poznatky z oblasti projektového manažmentu, ktorý aj vyučujem. Mohli sme to aplikovať do koordinácie technických odborníkov aj v komunikácii medzi akademickým prostredím a biznis partnerom. Boli sme zapojení už od začiatku pri príprave dokumentácie pred schválením projektu, aby sme nastavili jeho potenciál tak, aby priniesol deklarovaný efekt. Hľadáme tam prepojenie napríklad pre záverečné práce alebo projektovú výučbu študentov.

Majú už študenti témy naviazané na projekt?

Áno, riešia sa celý čas a je to blízka téma aj nášmu vedúcemu katedry, profesorovi Kubinovi. Organizácie majú naozaj záujem dozvedieť sa viac o posilnení kybernetickej bezpečnosti, vnímajú to ako kľúčovú prioritu.

Prečo je projekt potrebný pre verejnú správu alebo podniky?

Podnikom je poskytnuté konkrétne riešenie, ktoré majú predpripravené a nemusia začínať od nuly pri rozmýšľaní nad zabezpečením. Projekt im poskytne návrh, ako by to bolo najideálnejšie s dostupnými nekomerčnými riešeniami, takže ani finančná náročnosť nie je vysoká. Malé podniky často nemajú vnútornú expertízu ani ľudí. Projekt prináša veľký prehľad komponentov a firmy nemusia samy skúšať, či sú softvéry kompatibilné. Stále je tam dôležitý ľudský faktor – zamestnanci môžu byť rizikom aj výhodou, a výstupy projektu ponúkajú aplikovateľné riešenia s nižšími nákladmi práve pre tie organizácie, ktoré by inak support okolo veľkých riešení finančne nezvládli.

Aké riziká projekt ovplyvňovali?

Pri podpore projektového riadenia sme sa zaoberali identifikáciou a riadením rizík, aby sme minimalizovali negatívne dopady. Jedným z rizík bola neefektívna komunikácia medzi viacerými partnermi. Napríklad zladiť časový harmonogram – na univerzite sú v lete povinné dovolenky, a zrazu na naplánovaný míting prišli z 20 ľudí traja. Tiež kapacity ľudí sa líšia podľa toho, či je semester alebo nie. Museli sme sledovať nadväznosť výstupov v pracovných balíkoch, aby nikto nebrzdil ďalších členov tímu.

Čo bolo najnáročnejšie pri príprave odborných výstupov?

Formálne požiadavky sú jasne definované, tam problém nebol. Najkritickejší je samotný výskum. Pokiaľ nemáme dáta a zistenia, nemôžeme tvoriť publikácie do renomovaných časopisov. Museli sme s predstihom plánovať, kde sa výskum odpublikuje (konferencie, časopisy), pretože proces recenzovania sa nedá urýchliť.

Nemôžeme sa spoliehať na to, že výstupy dobehneme na konci projektu, museli sme na tom robiť paralelne a mať aj záložný plán (backup), keby niektorý výstup nevyšiel.

Čo vám projekt dal osobne alebo ľudsky?

V technickej stránke sme sa museli zorientovať v konkrétnych výrazoch a nástrojoch, niekedy sme si kľúčové slová rýchlo vyhľadávali na mobile, aby sme téme rozumeli. Z ľudskej stránky to bola koordinácia s viacerými partnermi; bol to náš prvý veľký projekt, kde sme na dennej báze kooperovali s partnerom z praxe. Posilnilo to aj vzťahy a rešpekt voči expertíze kolegov z inej katedry, pretože IT oblasť sa dynamicky mení.

Prekvapilo vás niečo na projekte?

Prekvapilo nás administratívne pozadie veľkých ganttových schém a požiadavky na výkazníctvo a priebežné monitorovanie zo strany agentúr. Pozitívne nás však prekvapila ochota a sila ľudí, ktorí sa v čase časového tlaku zomkli a boli schopní dodať výstupy. Prejavili veľkú flexibilitu a iniciatívu.

Čo by ste v budúcnosti robili inak?

Hneď na začiatku by sme si stanovili systém pravidelného vykazovania. Ešte lepšie by sme zladili vnútorné sledovanie progresu s oficiálnymi termínmi agentúry, aby sme dokumentáciu nemuseli robiť duplicitne alebo ju narýchlo updatovať.

Ktorý výstup z INNOSOCu je podľa vás najdôležitejší?

Najdôležitejší je samotný návrh a otestovanie – proof of concept. To, že sa to dá naozaj reálne aplikovať do praxe s navrhnutou architektúrou a nie je to len riešenie ‚do šuflíka', ale niečo udržateľné pre reálnych klientov a organizácie."

Príloha 25 – Rozhovor s Ing. Martinom Mičiakom, PhD.

Moje meno je Martin Mičiak, som z Katedry manažérskych teórií na Fakulte riadenia informatiky, som odborný asistent a v rámci projektu INNOSOC som bol aj výskumným pracovníkom aj súčasťou podpory projektového riadenia. Témou projektu INNOSOC je oblasť kybernetickej bezpečnosti a možnosti ako posilniť túto bezpečnosť v organizáciách aj s nižšími celkovými nákladmi na základe open riešení. Pri každom projekte je dôležité aby jeho výstupy v oblasti vedy boli publikované v renomovaných vydavateľstvách a v indexovaných časopisoch alebo konferenciách v dôležitých databázach pretože to dodáva celkovým výstupom aj celému projektu dôležitosť, relevantnosť a tým pádom aj bude posilnené jeho ďalšie šírenie a vlastne povedomie v odbornej komunite aj v očiach verejnosti. Pri príprave každého výskumného výstupu ktorý má byť neskôr publikovaný je najnáročnejší samotný výskum, je potrebné prísť s myšlienkou a vlastne zmapovať si tú oblasť tak aby každý ďalší výstup ju ďalej rozširoval a reagoval na vlastne výskumnú medzeru, to čo v článkoch a v konferenciách je zachytené pod spojením research gap. Vždy je potrebné napasovať ten ďalší výstup na to aby naozaj prinášal v tej danej téme, ktorú ten článok alebo ten príspevok na konferenciu detailne skúma alebo rieši, tak aby priniesol niečo nové a tým pádom bol zaujímavý a vlastne komunita alebo aj ďalej verejnosť a prax mali záujem si takýto výstup otvoriť a prečítať. Projekt INNOSOC je zaujímavou kombináciou akademického a biznis prostredia a v rámci fakulty sa na ňom podieľajú dve katedry, ide o našu Katedru manažérskych teórií a Katedru informačných sietí. Čiže ide celkovo o veľmi dôležitú a zaujímavú spoluprácu, ktorá mi pomohla si ešte viac prehĺbiť prepojenie manažérskej a informatickej oblasti. Tiež mi to rozšírilo celkovo povedomie o dôležitej téme kybernetickej bezpečnosti a pomohlo mi to získať ďalšie praktické skúsenosti z oblasti podpory projektového riadenia."

Príloha 26 – Rozhovor s Ing. Dominikou Toman, PhD.

Moje meno je Dominika Toman, som odborný asistent na Katedre manažérskych teórií na Fakulte riadenia a informatiky a v rámci projektu INNOSOC zabezpečujem napríklad podporu projektového riadenia alebo koordináciu ľudí v tomto projekte.
Význam projektu z pohľadu verejnosti, či už odbornej alebo všeobecnej, by som popísala tak, že je to rozširovanie obzorov v rámci kybernetickej bezpečnosti, posúvanie základných informácií, ktoré sa týkajú týchto riešení a toho, ako pomôcť v tejto oblasti.
Čo sa týka odbornej praxe, ide o publikačnú činnosť, publikovanie informácií o kybernetickej bezpečnosti, čiže prehlbovanie tých informácií a znalostí. V rámci projektu boli postupne publikované mnohé články, nielen články, ale možno aj prezentované informácie na konferenciách. Či už išlo o čiastkové výstupy, ktoré sa týkali nejakého rešeršu, aké sú najvhodnejšie riešenia pre podporu kybernetickej bezpečnosti, alebo sa postupne publikovali aj výsledky týkajúce sa napríklad vhodných školení pre zamestnancov organizácií, ktoré si budú zlepšovať tú kybernetickú bezpečnosť, aby vedeli tieto riešenia možno ovládať.
V rámci projektu INNOSOC som sa dozvedela množstvo nových informácií, svoje zručnosti v oblasti riadenia a koordinácie som si v podstate zdokonalila a mohla som ich rozvíjať pri vytváraní jednotlivých výstupov, pri komunikácii s partnermi, či už z univerzity alebo z praxe.“

Príloha 27 – Rozhovor s prof. Ing. Milan Kubina, PhD.

Som profesor Kubina, pôsobím na Fakulte riadenia a informatiky, som vedúci Katedry manažérskych teórií a v rámci INNOSOC som spoluriešiteľ projektu, ale som aj zodpovedný riešiteľ, čiže sme dvaja kľúčoví riešitelia, keď to tak poviem, profesor Segeč a ja, plus kľúčoví riešitelia z našich partnerov, ako je BRAIN:IT. Ja viac-menej zodpovedám za komunikáciu medzi tímami, medzi partnermi a hlavne medzi vedeckou agentúrou.
Hlavná myšlienka projektu INNOSOC bolo, že žijeme v takej digitálnej dobe, všetci využívajú tieto technológie, kopec ľudí hľadá cesty, ako využiť nejaké systémové chyby alebo problémy v nezrovnalosti, keď to tak poviem všeobecne, v týchto aplikáciách a nabúrať sa do systémov, obohatiť sa. Čiže tento INNOSOC bol myslený hlavne pre malé firmy, verejnú správu, čiže obce, školy, keďže oni nemajú peniaze, aby sme im pomohli trošku, aby sa cítili bezpečnejšie v tom kybernetickom priestore.
Jedná sa o SOC centrum, čiže respektíve o nejaké nástroje, ktoré by mali riešiť problematiku kybernetickej bezpečnosti a prevádzky IP sietí. Vo finále by to mala byť cloudová služba, tento projekt je na úrovni TRL3 a my sa snažíme urobiť dizajn tohto produktu tak, aby to bolo cloudové, multitenantné a aby boli splnené náležitosti, aby to riešenie nebolo finančne náročné pre budúcich kvázi odberateľov.
Ja ako nejaký stredný manažér, keďže som vedúci katedry, vnímam, že spolupráca medzi univerzitnou sférou a praxou je veľmi dôležitá a snažím sa motivovať svojich kolegov, aby sa čo najviac prepájali s praxou, či už pomocou diplomových alebo bakalárskych prác, alebo cez vyžiadané prednášky. Som veľmi rád, že také spoločnosti ako BRAIN:IT radi spolupracujú s fakultou riadenia, podporujú aj fakultu aj študentov a myslím, že tá synergia je na oboch stranách veľmi dobrá.“