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

1 Úvod 4

2 Čiastkové ciele osvetových aktivít 4

2.1 Zdieľanie výstupov a informácií prostredníctvom webovej platformy 4

2.2 Informovanie laickej verejnosti o dôležitosti kybernetickej bezpečnosti a potenciálu projektu INNOSOC 5

2.3 Popularizácia témy a zvýšenie digitálnej gramotnosti medzi študentmi 5

3 Popis segmentov pre osvetové aktivity 6

3.1 Odborná verejnosť 6

3.2 Široká/laická verejnosť 6

3.3 Potenciálni zákazníci 6

3.4 Študenti stredných škôl 7

3.5 Študenti vysokých škôl 7

4 Spôsoby oslovenia a komunikačné nástroje 7

4.1 Webová stránka 7
4.1.1 Realizované aktivity 8

4.2 Sociálne siete 18
4.2.1 Východiská komunikačnej stratégie 18
4.2.2 Hlavné komunikačné nástroje 18
4.2.3 Obsahový plán 19
4.2.4 Realizované aktivity 20

4.3 Popularizačné texty 38
4.3.1 Realizované aktivity 38

4.4 Audiovizuálny obsah 44
4.4.1 Realizované aktivity 45

4.5 Promo materiály 47
4.5.1 Realizované aktivity 48

5 Zoznam zdrojov 50

6 Prílohy 53

Prílohe 1 – Článok: Stretnutie partnerov 15.7.2025 53

Príloha 2 – Článok: Základy projektu INNOSOC: Rozhovor s Ing. Michalom Papučíkom 53

Príloha 3 – Článok: Rozhovor s prof. Ing. Pavlom Segečom, PhD.: Kybernetická bezpečnosť už nie je len témou pre veľké firmy 54

Príloha 4 – Článok: Študentská udalosť FRIčkovica – 8.októbra 55

Príloha 5 – Oznam o konaní sympózia INNOSOC 55

Príloha 6 – Článok o vyhlásení víťaza súťaže o iPad 55

Príloha 7 – Článok: Prezentácia projektu INNOSOC na študentských raňajkách 55

Príloha 8 – Článok o prezentácii projektu na fakulte Aplikovanej informatiky na Univerzite Tomáše Báti v Zlíne 55

Príloha 9 – Článok o prezentácii projektu INNOSOC na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici 56

Príloha 10 – Článok: Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami 56

Príloha 11 – Článok: Security Operations Center: čo to je a ako chráni vašu firmu? 58

Príloha 12 – Článok: Spoznajte najčastejšie hrozby internetu pre mladých: Možnosti prevencie a ochrany 59

Príloha 13 – Článok: Čo je to cloud a na čo slúži: Základné typy a výhody cloudového úložiska 61

Príloha 14 – Článok: Počítačová bezpečnosť a ochrana dát – princípy a praktické príklady 63

Príloha 15 – Rozhovor s Ing. Michalom Papučíkom 65

Príloha 16 – Rozhovor s prof. Ing. Pavlom Segečom, PhD. 66

1 Úvod

Dokument obsahuje rozpracovanú verziu návrhu stratégie pre realizáciu osvetových aktivít. Hlavným cieľom stratégie je vybudovať povedomie o projekte INNOSOC ako o európskom technologickom projekte s významom pre kybernetickú bezpečnosť a digitálnu suverenitu. Projekt má byť vnímaný ako inovatívny, dôveryhodný a otvorený nástroj pre prevenciu a riadenie kybernetických hrozieb.

Dôraz bude kladený na edukáciu, komunitnú interakciu a podporu prijatia technológie nielen medzi odborníkmi, ale aj medzi mladými talentmi a širokou verejnosťou.

Predpokladané cieľové publikum osvetových aktivít je možné rozdeliť do piatich základných segmentov:

- odborná verejnosť,
- široká/laická verejnosť,
- potenciálny zákazníci,
- študenti stredných škôl,
- študenti vysokých škôl.

Každý z daných segmentov je špecifický a vyžaduje si individuálny mix komunikačných kanálov pre šírenie povedomia a zároveň aj špecifickú myšlienku komunikácie.

2 Čiastkové ciele osvetových aktivít

Vzhľadom na široké spektrum cielených segmentov a najmä na rôzne komunikačné myšlienky, ktoré im majú byť komunikované bolo definovaných niekoľko čiastkových cieľov osvetových aktivít.

2.1 Zdieľanie výstupov a informácií prostredníctvom webovej platformy

Jedným z hlavných cieľov osvetových aktivít v rámci projektu INNOSOC je vybudovanie otvorenej digitálnej platformy, ktorá bude slúžiť ako priestor pre zdieľanie výsledkov, poznatkov a výstupov projektu. Informácie na webovej stránke budú určené pre viaceré segmenty. Zároveň však pôjde o nosný nástroj zdieľania odborných znalostí pre komunikáciu s odbornou verejnosťou.

Táto platforma bude verejne dostupná a umožní rôznym cieľovým skupinám, od odborníkov až po laikov, jednoduchý prístup k dôležitým informáciám a podkladom. Webová stránka projektu sa stane centrálnym miestom, kde budú publikované záverečné správy, technické dokumenty, návody, metodiky, vizualizácie aj výskumné dáta.

Dôležitou súčasťou bude možnosť spätnej väzby a aktívnej interakcie zo strany návštevníkov, čím sa podporí obojsmerná komunikácia medzi riešiteľmi projektu a verejnosťou. Platforma bude zároveň miestom, kde sa budú priebežne uverejňovať nové poznatky z experimentov a testovania, pričom dôraz sa bude klásť na transparentnosť a využiteľnosť výsledkov.

Tento prístup odráža princípy otvorenej vedy a umožňuje, aby boli výstupy projektu znova použité vo vede, vývoji alebo výučbe. Cieľom je vytvoriť ekosystém, v ktorom výskum neslúži len ako jednorazový výstup, ale ako trvalo udržateľný základ pre ďalší rozvoj v oblasti kybernetickej bezpečnosti a cloudových riešení.

2.2 Informovanie laickej verejnosti o dôležitosti kybernetickej bezpečnosti a potenciálu projektu INNOSOC

Rastúce kybernetické hrozby priniesli nutnosť informovať širokú, laickú verejnosť o vhodných nástrojoch kybernetickej bezpečnosti. Je preto nevyhnutné aby bola verejnosť oboznámená s tým ako projekt INNOSOC prispieva k ochrane digitálneho priestoru práve pre členov verejnosti, pre ktorých boli existujúce riešenia finančne nedostupné.

Vzhľadom na to, že väčšina populácie získava informácie online, rozhodli sme sa prioritne využiť webovú stránku a sociálne siete ako hlavné komunikačné kanály. Webová stránka umožňuje centralizovane a prehľadne prezentovať ciele, výstupy, vizualizácie aj novinky z projektu zrozumiteľným a edukatívnym spôsobom. Zjednodušený jazyk tak bude možné viesť paralelne s tým odborným, ktorý nadväzuje na predošlý čiastkový cieľ.

Sociálne siete zas ponúkajú interaktívnu formu komunikácie, cez ktorú môžeme osloviť rôzne skupiny občanov a vytvárať dialóg o bezpečnosti na internete. Ich silnou stránkou je rýchlosť šírenia obsahu, vizuálna zaujímavosť pre verejnosť a možnosť zapájať publikum do kampaní, kvízov či diskusií. Vďaka týmto nástrojom môžeme efektívne šíriť povedomie o význame kybernetickej bezpečnosti, rizikách hrozieb aj výhodách inteligentných riešení, aké prináša INNOSOC. Týmto spôsobom sa snažíme prispieť k vyššej digitálnej gramotnosti verejnosti a zároveň zvýšiť spoločenský dopad projektu.

2.3 Popularizácia témy a zvýšenie digitálnej gramotnosti medzi študentmi

Jedným z čiastkových cieľov projektu INNOSOC je popularizácia témy kybernetickej bezpečnosti a zároveň zvyšovanie digitálnej gramotnosti medzi študentmi stredných a vysokých škôl. Osvetové aktivity budú realizované najmä prostredníctvom webovej stránky projektu a sociálnych sietí, ktoré umožnia efektívne osloviť študentov v prostredí, ktoré je im blízke a prirodzené. Tieto digitálne kanály poskytnú priestor na zverejňovanie popularizačných článkov, návodov, videí a krátkych interaktívnych príspevkov, ktoré budú zrozumiteľne a pútavo vysvetľovať základné princípy kyberbezpečnosti, hrozby digitálneho sveta aj spôsoby ich riešenia.

Významným prínosom projektu je aj to, že umožní Univerzite Žilinská v Žiline, konkrétne Fakulte riadenia a informatiky (UNIZA FRI), vybudovať funkčné SOC riešenie ako súčasť výučby, ktoré sa stane praktickým nástrojom na rozvoj zručností študentov. Výučba bude prebiehať formou projektovo a problémovo orientovaného vzdelávania, vďaka čomu študenti získajú nielen teoretické poznatky, ale aj reálnu skúsenosť s navrhovaním, testovaním a implementáciou bezpečnostných riešení v cloudovom prostredí.

Cieľom je výrazne zvýšiť počet študentov zapojených do praktickej výučby v oblastiach kyberbezpečnosti a cloud computingu a motivovať ich k ďalšiemu štúdiu alebo výskumnej činnosti v tejto oblasti. Pravidelným zverejňovaním obsahu na sociálnych sieťach ako sú napríklad infografiky, kvízy, ukážky z vývoja alebo rozhovory s odborníkmi sa buduje vzťah so študentmi a zvyšuje ich záujem o danú tému.

INNOSOC tak vytvára nielen vzdelávaciu a výskumnú infraštruktúru, ale aj živý a otvorený komunikačný kanál so študentskou komunitou. Projekt tým zároveň podporuje vznik nových vedecko-výskumných aktivít a spĺňa charakteristiky budúceho riešenia s komerčným potenciálom, ktoré sa už v čase vývoja stáva súčasťou edukačného a osvetového prostredia.

3 Popis segmentov pre osvetové aktivity

Každý zo segmentov osvetových aktivít prináša individuálne potreby komunikácie a priestor pre vhodné zacielenie.

3.1 Odborná verejnosť

Odborná verejnosť zahŕňa IT profesionálov, bezpečnostných analytikov, výskumníkov a akademických pracovníkov, ktorí sa venujú kybernetickej bezpečnosti, cloudu alebo umelej inteligencii.

Táto skupina je primárnym príjemcom odborných výstupov projektu najmä pokiaľ ide o technickú dokumentáciu, výskumné články, algoritmy a architektúru SOC riešenia. Vďaka odborným výstupom, open-access publikáciám a sympóziám získavajú príležitosť na odbornú diskusiu, spätnú väzbu a prepájanie výskumných iniciatív.

Projekt INNOSOC ponúka tejto skupine aj možnosť participácie na vývoji cez spätno-väzbové mechanizmy na webstránke. Významným benefitom je prístup k otvoreným výstupom, ktoré môžu využiť vo vlastnom výskume alebo vývoji. Projekt týmto cieľovým skupinám poskytuje kvalitný podklad na vedeckú spoluprácu a inováciu.

3.2 Široká/laická verejnosť

Široká verejnosť predstavuje občanov bez špecializácie v IT, ktorí však čoraz častejšie čelia kybernetickým rizikám pri bežnom používaní internetu a digitálnych služieb.

Projekt INNOSOC má ambíciu zvyšovať povedomie o význame kybernetickej bezpečnosti aj medzi touto skupinou. Webová stránka a sociálne siete budú slúžiť ako nástroj na popularizáciu témy pomocou popularizačných článkov, videí, infografík či animácií.

Cieľom je vysvetliť základné pojmy ako „SOC“, „anomália“, „cloud“, „AI“ a ukázať, ako tieto technológie chránia ich každodenné digitálne aktivity. Dôraz sa kladie na zrozumiteľnosť, vizualizáciu a praktické príklady. Projekt zároveň prispieva k zvyšovaniu digitálnej gramotnosti, čo je v súlade s európskymi aj národnými stratégiami. Aktivizovaním tejto skupiny môže projekt INNOSOC dosiahnuť širší spoločenský dopad a podporiť informované digitálne správanie.

3.3 Potenciálni zákazníci

Potenciálnymi zákazníkmi projektu sú najmä malé a stredné podniky (MSP), väčšie firmy, ako aj organizácie verejnej správy, ktoré čelia rastúcim nárokom na ochranu IT infraštruktúry a dát.

INNOSOC im ponúka inovatívne SOC riešenie dostupné ako služba (SOCaaS), ktoré je flexibilné, škálovateľné a efektívne. Zákazníci ocenia výhody multitenantnej architektúry, predikčného monitoringu a automatizovanej detekcie hrozieb založenej na AI.

Primárnou zvolenou metódou pre oslovenie potenciálnych zákazníkov bol zvolený direct sales prostredníctvom e-mailu, telefonického oslovenia a osobnej komunikácie. Podpornú stránku oslovovania však budú tvoriť existujúce osvetové aktivity v podobe sociálnych sietí a web stránky.

Webová stránka projektu bude obsahovať sekciu venovanú komerčnému potenciálu a možnostiam využitia riešenia. Cieľom je budovať dôveru a pripraviť trh na budúce nasadenie platformy.

Pre úspešné oslovenie zákazníkov sú zároveň potrebné aj podporné výstupy určené na osvetové aktivity ako sú brožúry, letáky, roll-upy a podobne.

3.4 Študenti stredných škôl

Táto skupina predstavuje budúcich odborníkov, ktorých je potrebné včas zaujať témami bezpečnosti a moderných technológií.

Projekt INNOSOC bude prostredníctvom sociálnych sietí, blogov a krátkych videí šíriť populárno-náučný obsah, ktorý bude vysvetľovať základy kybernetickej bezpečnosti, princípy ochrany dát a úlohu umelej inteligencie.

Dôraz sa bude klásť na zrozumiteľnosť, hravosť a vizuálnu stránku formou infografík, kvízov a prípadne gamifikovaných prvkov. Cieľom je vzbudiť záujem o IT a kyberbezpečnosť ako potenciálnu študijnú alebo kariérnu cestu. Súčasťou aktivít môžu byť aj online súťaže, zapojenie do popularizačných kampaní alebo workshopy v spolupráci so školami. Projekt chce týmto študentom ukázať, že kyberbezpečnosť nie je len pre odborníkov, ale téma, ktorej porozumie každý a ktorá je v dnešnej dobe nevyhnutná.

3.5 Študenti vysokých škôl

Študenti vysokých škôl technického a informatického zamerania patria medzi hlavné cieľové skupiny INNOSOC projektu. Cieľom je nielen zvýšiť ich povedomie o bezpečnostných technológiách, ale predovšetkým ich aktívne zapojiť do vývoja, testovania a učenia sa prostredníctvom projektovo a problémovo orientovanej výučby.

Platforma INNOSOC poskytne reálne SOC riešenie využiteľné v praktickej výučbe, čím študenti získajú cenné zručnosti v oblasti cloudových architektúr, monitoringu a AI-based detekcie hrozieb. Osvetové aktivity, vedené prostredníctvom webu a sociálnych sietí, im budú poskytovať technický obsah, tutoriály, príklady implementácií a odborné komentáre k riešeniam.

Vytvorí sa aj priestor pre spätnú väzbu, diskusiu či zapojenie do súťaží a záverečných prác. Projekt tak prispieva nielen k zvyšovaniu odbornosti, ale aj k lepšej pripravenosti absolventov na potreby trhu práce a ďalší výskum.

4 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.

4.1 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.

Do budúcnosti je ambíciou, aby 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.

4.1.1 Realizované aktivity

4.1.1.1 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,**
- **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 budú zverejňované blogové články, popularizačné články ako aj všetky novinky, ktoré sa týkajú realizovaných aktivít, stretnutí či publikovaných indexových článkov a publikácií.

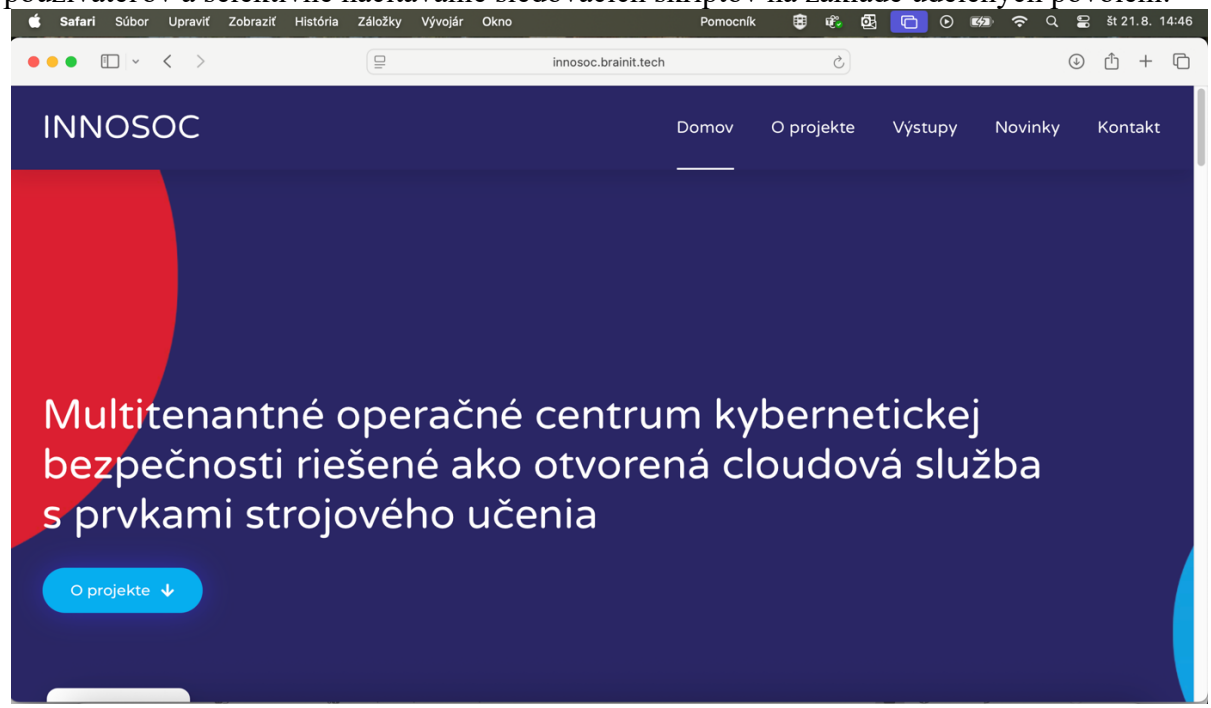
Poslednou dostupnou sekciou je „Kontakt“, kde má používateľ prístupný formulár v prípade otázok.

Pre efektívne zastrešenie osvetových aktivít bolo nutné na web implementovať vybrané analytické nástroje. Implementácia analytických nástrojov na webovej stránke projektu INNOSOC predstavuje kľúčový prvok pre efektívne meranie dopadu osvetových aktivít a optimalizáciu komunikačnej stratégie. Analytické nástroje umožnia riešiteľom projektu prijímať dátami podložené rozhodnutia o ďalšom smerovaní osvetových aktivít a zároveň poskytnú objektívne metriky pre hodnotenie úspešnosti jednotlivých komunikačných kanálov.

Základným analytickým nástrojom je Google Analytics 4, ktorý poskytuje komplexný prehľad o návštevnosti, zdrojoch návštevníkov, demografických charakteristikách používateľov a ich správaní na stránke. Google Tag Manager slúži ako centrálny systém pre správu všetkých sledovacích kódov, čo umožní flexibilné a rýchle úpravy bez potreby zásahov do kódu stránky.

Google Search Console poskytuje dôležité informácie o výkonnosti stránky vo vyhľadávačoch Google, vrátane pozícií kľúčových slov a chýb indexovania. Ahrefs je využívaný pre komplexnú SEO analýzu, sledovanie backlinkov a monitorovanie pozícií pre relevanté kľúčové slová v oblasti kybernetickej bezpečnosti.

Implementácia analytických nástrojov je realizovaná v súlade s GDPR nariadeniami a obsahuje transparentné informovanie používateľov o zbere dát prostredníctvom cookie bannerov a privacy policy. Google Tag Manager umožňuje jednoduchú správu súhlasov používateľov a selektívne načítavanie sledovacích skriptov na základe udelených povolení.

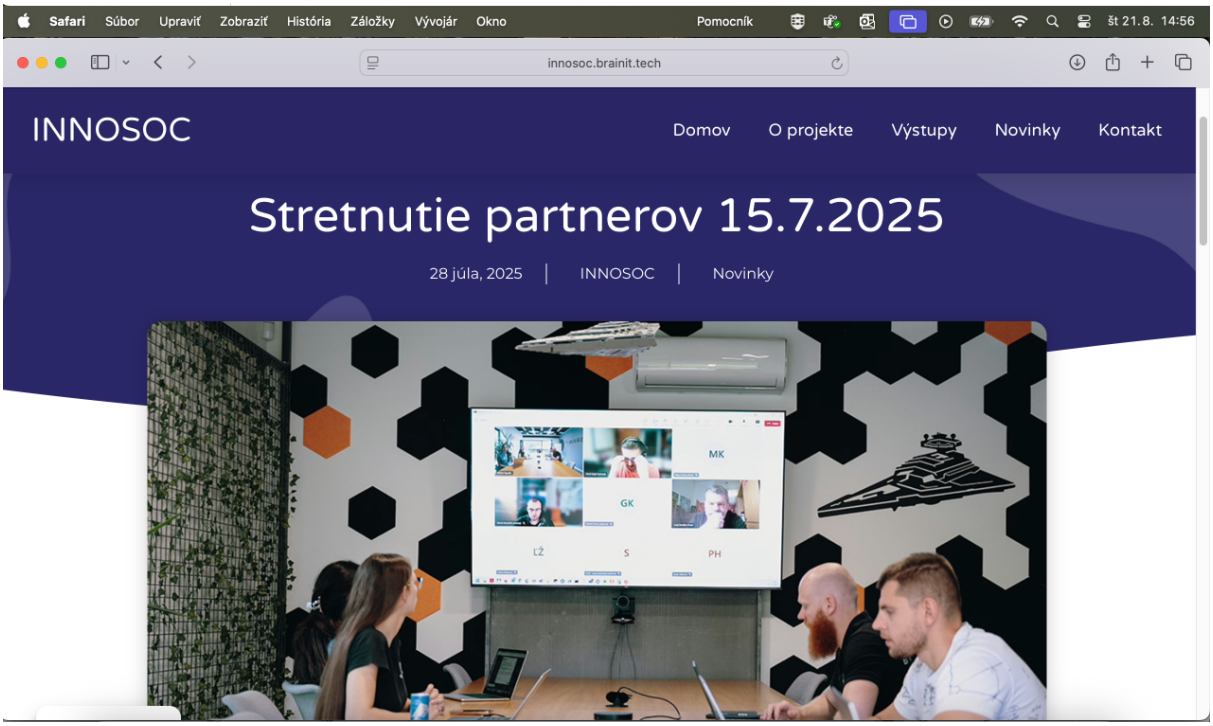


Obrázok 1: Náhľad úvodnej stránky INNOSOC, Zdroj: (BRAIN:IT, 2025)

4.1.1.2 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

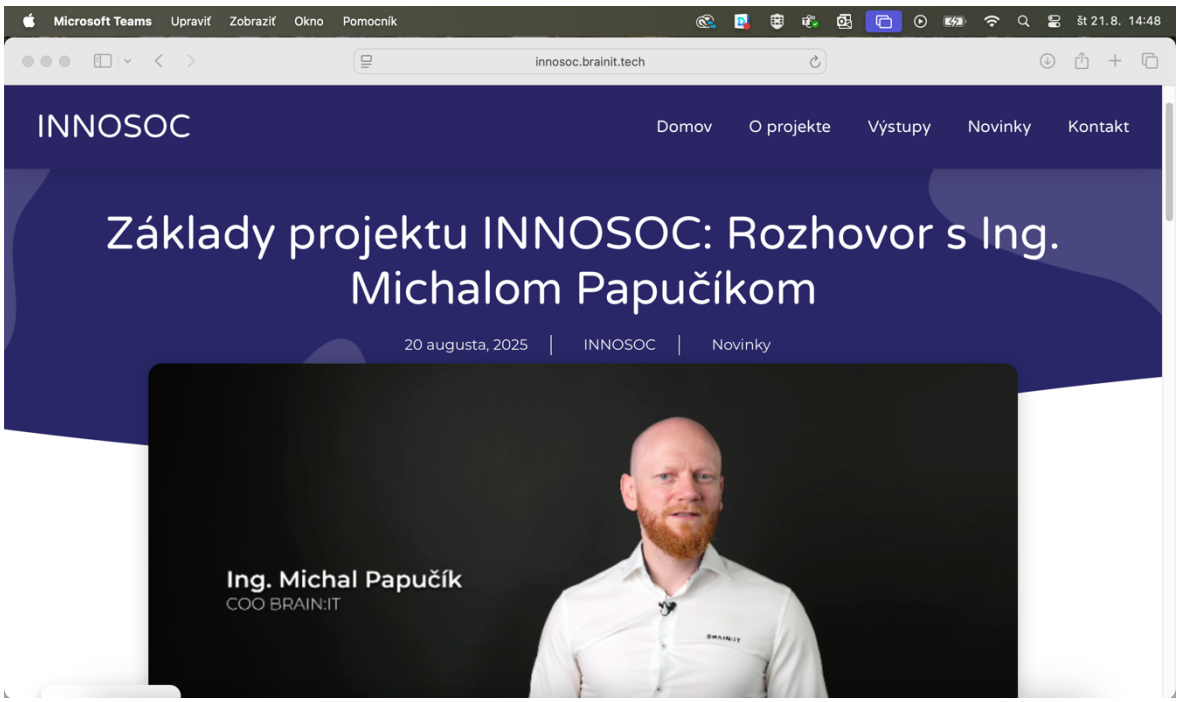


Obrázok 2: Článok na webovej stránke INNOSOC: Stretnutie partnerov 15.7.2025, Zdroj: (BRAIN:IT, 2025)

4.1.1.3 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)

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

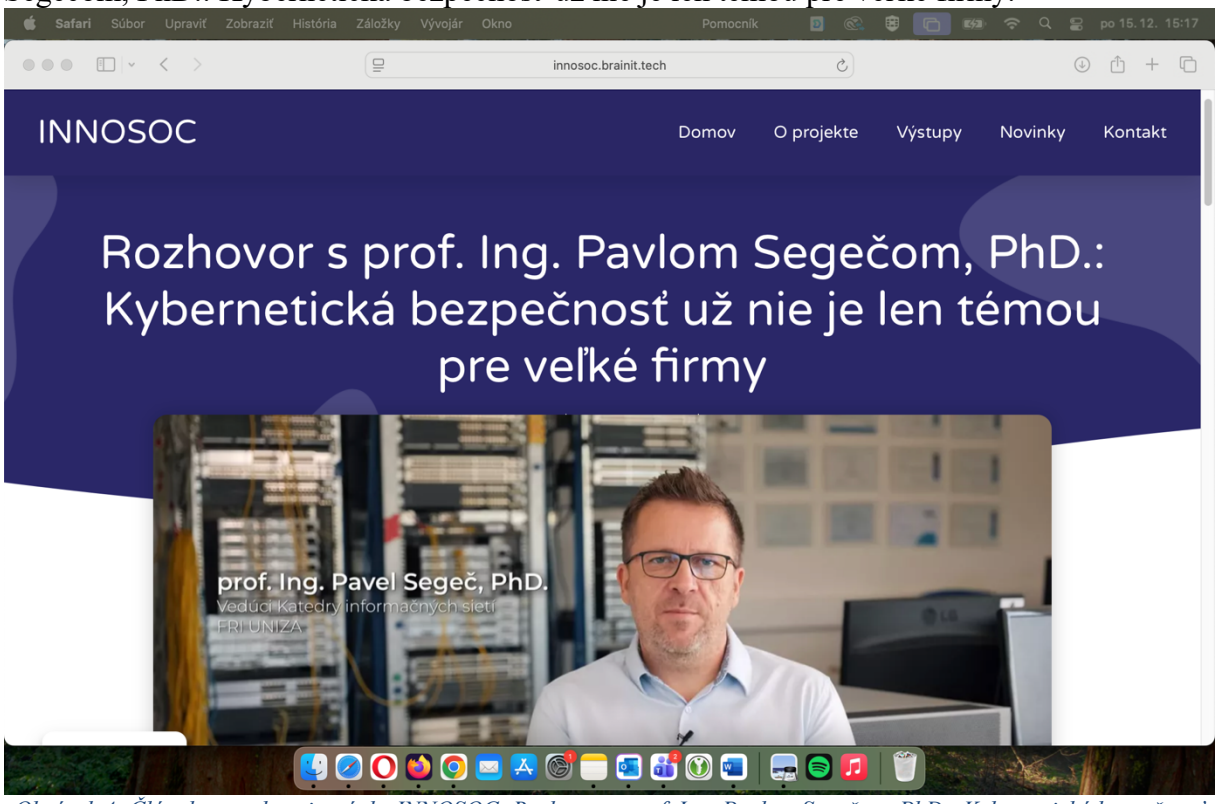
V rámci projektu bol dňa realizovaný a publikovaný odborný rozhovor s prof. Ing. Pavlom Segečom, PhD., vedúcim Katedry informačných sietí na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline (UNIZA), ktorý pôsobí ako kľúčový vedecko-výskumný pracovník projektu. Cieľom rozhovoru bolo priblížiť 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)

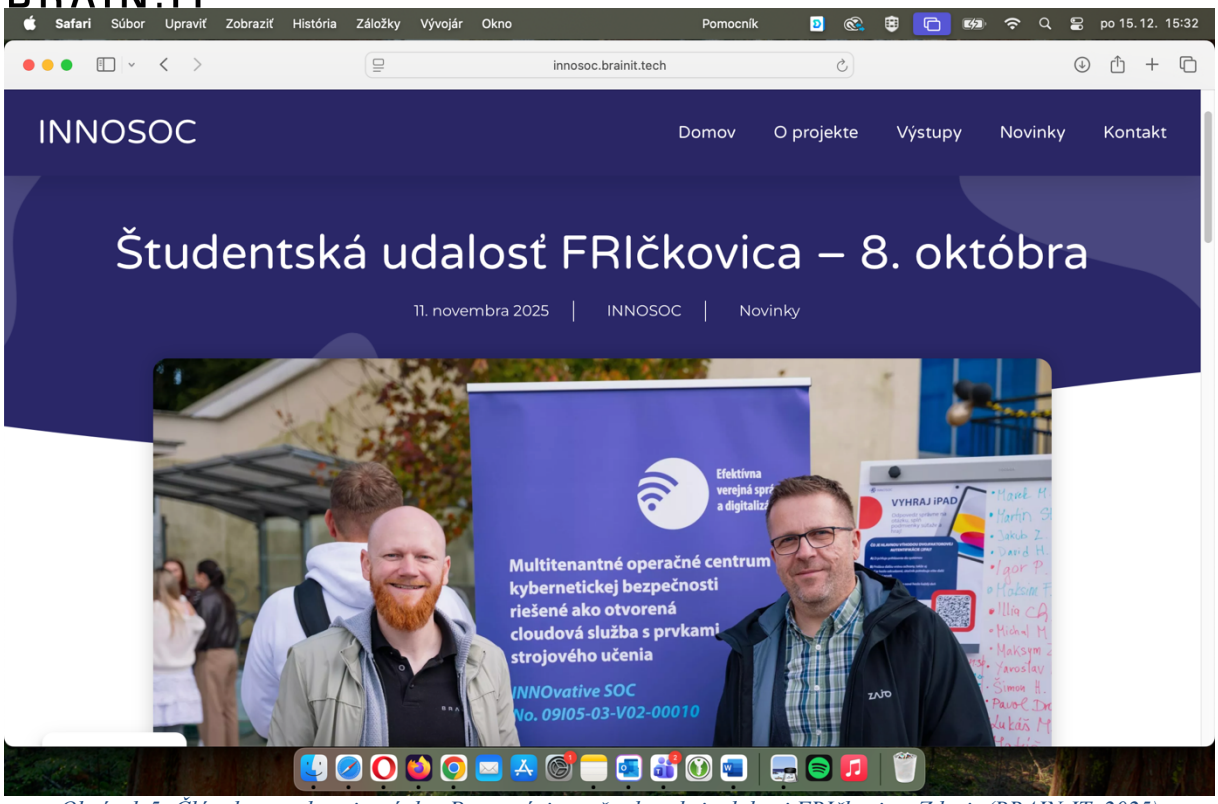
4.1.1.5 Článok o prezentovaní projektu INNOSOC na študentskej udalosti FRIčkovica

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.

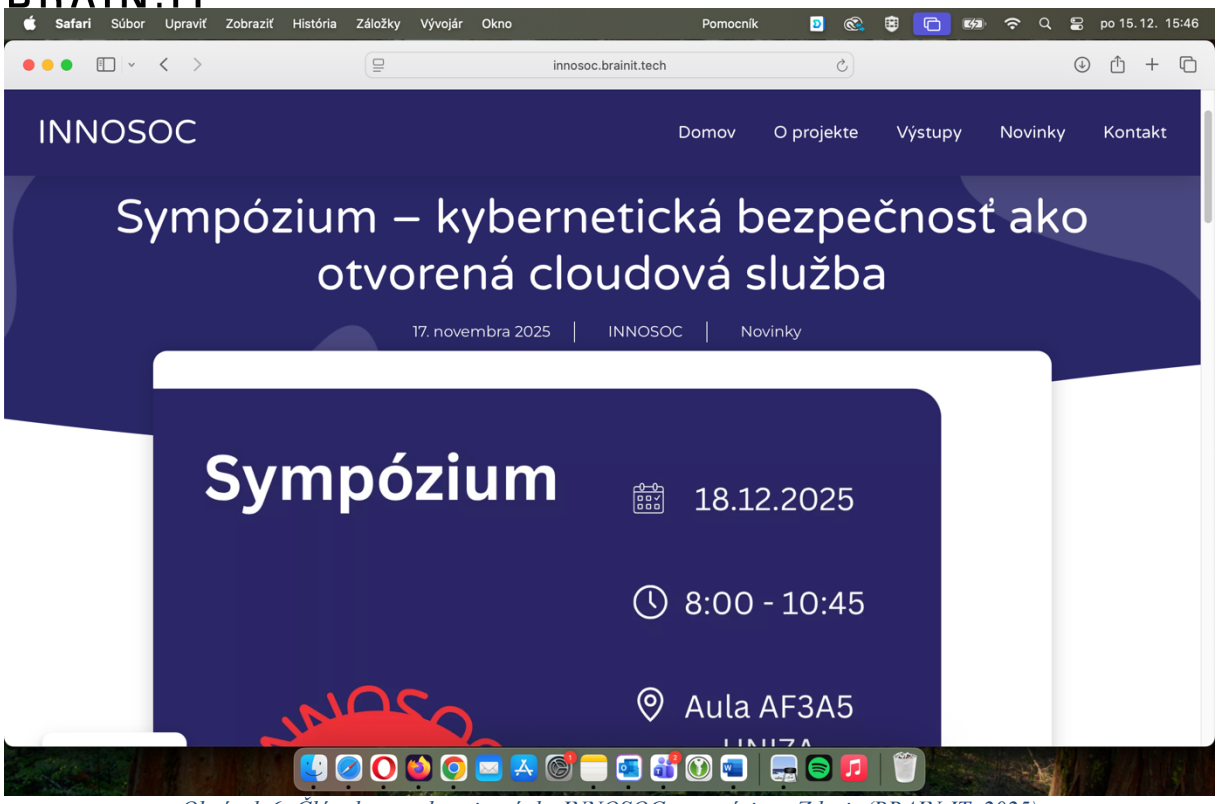


Obrázok 5: Článok na webovej stránke: Prezentácia na študentskej udalosti FRIčkovica, Zdroj: (BRAIN:IT, 2025)

4.1.1.6 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 je 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.

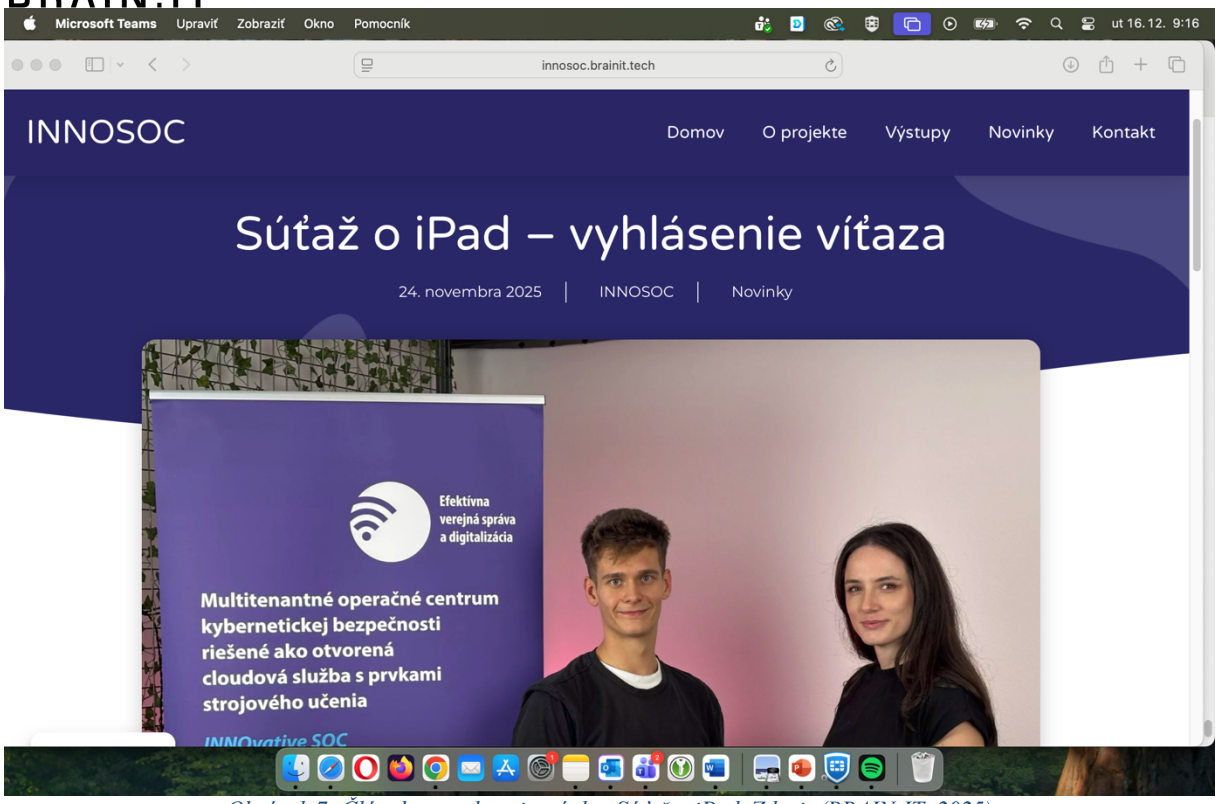


Obrázok 6: Článok na webovej stránke INNOSOC: sympózium, Zdroj: (BRAIN:IT, 2025)

4.1.1.7 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)

4.1.1.8 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)

4.1.1.9 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)

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

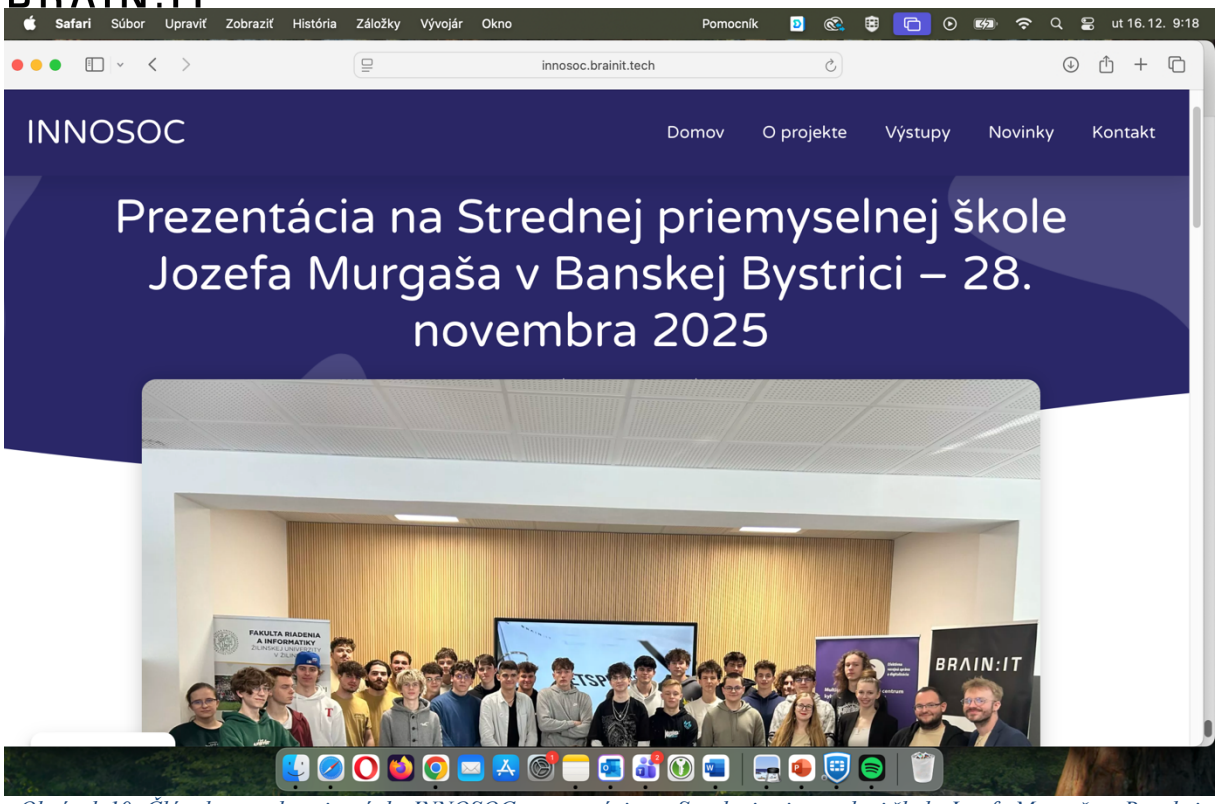
Dňa 12. decembra bol v sekcii „Novinky“ zverejnený článok, ktorý komunikuje prezentáciu projektu INNOSOC na Strednej priemyselnej škole Joefa Murgaša v Banskej Bystrici dňa 29. Novembra 2025. Cieľom aktivity bolo priblížiť projekt INNOSOC žiakom strednej školy, vysvetliť základné princípy kybernetickej 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)

4.2 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 – sa kľúčovým aspektom propagácie stáva 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.

4.2.1 Východiská komunikačnej stratégie

Cieľovou skupinou komunikácie nie sú len technologickí partneri alebo zákazníci. Dôležitou skupinou sú podľa dokumentu „Opis projektu“ aj:

- malé a stredné podniky bez interných IT oddelení,
- zástupcovia verejnej správy (školy, obce, inštitúcie),
- študenti a absolventi v oblasti informatiky,
- technologickí nadšenci a komunita v oblasti kybernetickej bezpečnosti,
- širšia laická verejnosť zaujímajúca sa o bezpečnosť v digitálnom priestore.

Z tohto dôvodu budú zvolené komunikačné kanály s rôznou úrovňou odbornosti, formy výstupov a jazykového štýlu. Obsah bude rozdelený do kategórií podľa typu cieľového segmentu, napr. odborný obsah pre LinkedIn, vizuálny a edukačný obsah pre Instagram.

4.2.2 Hlavné komunikačné nástroje

Na propagáciu môže byť použitých niekoľko platforiem, ktoré reflektujú diverzitu cieľových skupín.

Jedným z hlavných pilierov komunikačnej stratégie projektu môže byť LinkedIn profil spoločnosti BRAIN:IT, ktorý ma viac než 4000 sledujúcich. Ide o profesionálne orientovaný komunikačný kanál, zameraný najmä na B2B segment a odbornú komunitu. Prostredníctvom tohto profilu môžu byť publikované odborné príspevky, príspevky prezentujúce iné podporné aktivity spojené s projektom INNOSOC a poznatky nadobudnuté v zmysle realizovaného projektu. Cieľom je osloviť firemných partnerov, odbornú verejnosť a rozhodovacích aktérov v oblasti technológií a verejnej správy, čím sa súčasne posilní dôveryhodnosť projektu a jeho odborná legitimita.

Popri formálnom LinkedIn profile je dôležitým nástrojom aj Instagramový účet spoločnosti BRAIN:IT s 1000 sledujúcimi. Tento kanál má vizuálne a menej formálne zameranie, vďaka čomu sa hodí na prezentáciu aktivít projektu, výstupov projektu a zdieľanie poznatkov nadobudnutých v zmysle realizovaného projektu. Tento kanál je orientovaný najmä na mladšiu generáciu odborníkov, technickú komunitu, širšiu verejnosť a študentov a absolventov informatiky, pričom napomáha budovaniu značky a zvyšovaniu povedomia o projekte v neodbornej sfére.

Na akademickej úrovni môže byť projekt komunikovaný prostredníctvom profilov fakulty, ktoré už dnes dosahujú vysokú mieru interakcie so študentskou komunitou. Instagramový účet @budmanazer, ktorý ma viac než 900 sledujúcich, predstavuje komunitno-akademický kanál pre sledujúcich prevažne z radov študentov a mladých profesionálov. Obsah bude zameraný na výstupy projektu a zdieľanie poznatkov nadobudnutých v zmysle realizovaného projektu. Cieľom je aktivizovať mladú cieľovú skupinu a ukázať im projekt ako príležitosť pre osobný a profesijný rast.

Zásah do technologicky orientovaného publika poskytuje aj Instagram profil @budfri s 1900 sledujúcimi. Tento profil cieli na študentov a absolventov Fakulty riadenia a informatiky, ako aj na širšiu IT komunitu. Obsah môže tvoriť najmä prehľad technických výstupov a príspevky mapujúce prepojenie výskumu s reálnou praxou. Významnou úlohou tohto kanála je posilňovanie odborného povedomia.

Komunikačnú stratégiu môže dopĺňa aj oficiálny LinkedIn profil fakulty Faculty of Management Science and Informatics, University of Žilina, ktorý je určený na formálnejšiu prezentáciu výskumných a vzdelávacích projektov smerom k akademickej a vedecko-výskumnej komunite a ktorý sleduje viac než 2000 používateľov. Prostredníctvom tohto kanála môžu byť publikované oficiálne oznámenia o pokroku projektu, zhrnutia výskumných výstupov, zapojenie do národných a medzinárodných iniciatív, ako aj ukážky spolupráce s priemyslom. Cieľom je zakotviť projekt v kontexte strategických inovácií fakulty a prezentovať ho ako súčasť jej výskumného portfólia.

Ďalším doplnkovým prvkom komunikačnej stratégie môže byť vytvorenie samostatných účtov projektu INNOSOC na platformách Instagram a LinkedIn. Tieto účty by mohli slúžiť ako centrálne komunikačné body pre prezentáciu všetkých aktivít projektu naprieč jeho životným cyklom – od výskumného zámeru cez vývojové etapy až po finálne implementácie a demonštrácie. Obsah týchto profilov môže byť štruktúrovaný tak, aby v chronologickej a tematicky prehľadnej forme zachytával kľúčové míľniky realizácie, informoval o priebežnom pokroku, komunikoval výsledky a prezentoval aplikovateľnosť riešení v rôznych typoch organizácií. Instagramový profil môže byť vizuálne ladený a orientovaný na rýchlu a interaktívnu komunikáciu s verejnosťou, zatiaľ čo LinkedIn môže plniť úlohu odbornej vývesky projektu s dôrazom na výskumné, technologické a legislatívne aspekty. Tieto kanály môžu doplniť komunikáciu partnerov projektu a umožnia uchovávať a prezentovať projektové výsledky aj po jeho oficiálnom ukončení.

4.2.3 Obsahový plán

Doplnkovým výstupom propagácie príspevkov na sociálnych sieťach bude obsahový plán, ktorý slúži na zabezpečenie konzistentnej, včasnej a profesionálnej komunikácie naprieč všetkými platformami.

Tento obsahový plán bude obsahuje tieto prvky:

- Kalendár publikácií
- Dátum publikovania
- Téma
- Kanál distribúcie (IG, LinkedIn, @budfri...)
- Zodpovedná osoba za vytvorenie, schválenie a publikovanie
- Stav príspevku (návrh – čaká na schválenie – pripravený – publikovaný)
- Odkazy na médiá a assety (názov súboru, umiestnenie v cloude, pripravený QR kód)

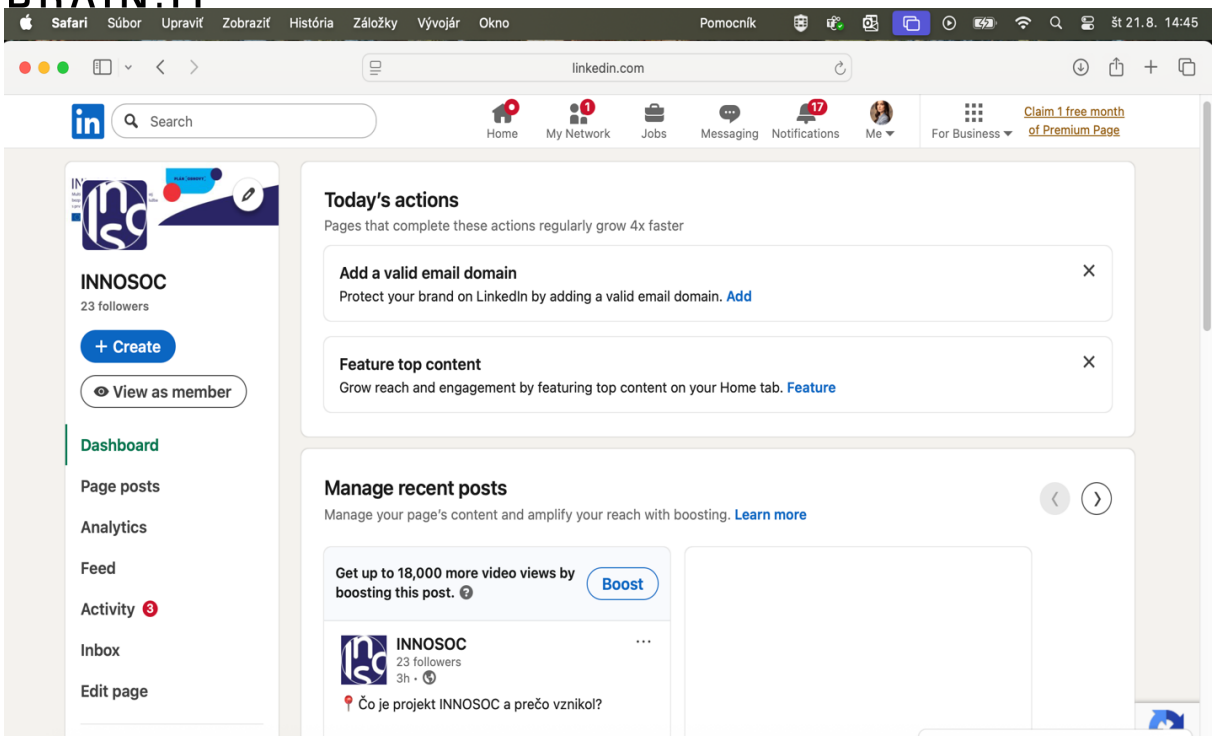
Excelový formát umožňuje efektívnu prácu v tíme, synchronizáciu úloh, spätné dohľadanie publikovaného obsahu a zároveň poskytne prehľad pri internom reportingu. Pravidelné kontroly umožňujú vyhodnotenie interakcií a optimalizáciu štýlu výstupov podľa toho, čo najlepšie funguje.

4.2.4 Realizované aktivity

4.2.4.1 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 bude zároveň komunikovať dlhšie odborné príspevky, články, bude slúžiť ako kanál na komunikáciu s odbornou verejnosťou. Povaha tejto sociálnej siete zabezpečí vysokú mieru dôveryhodnosti.

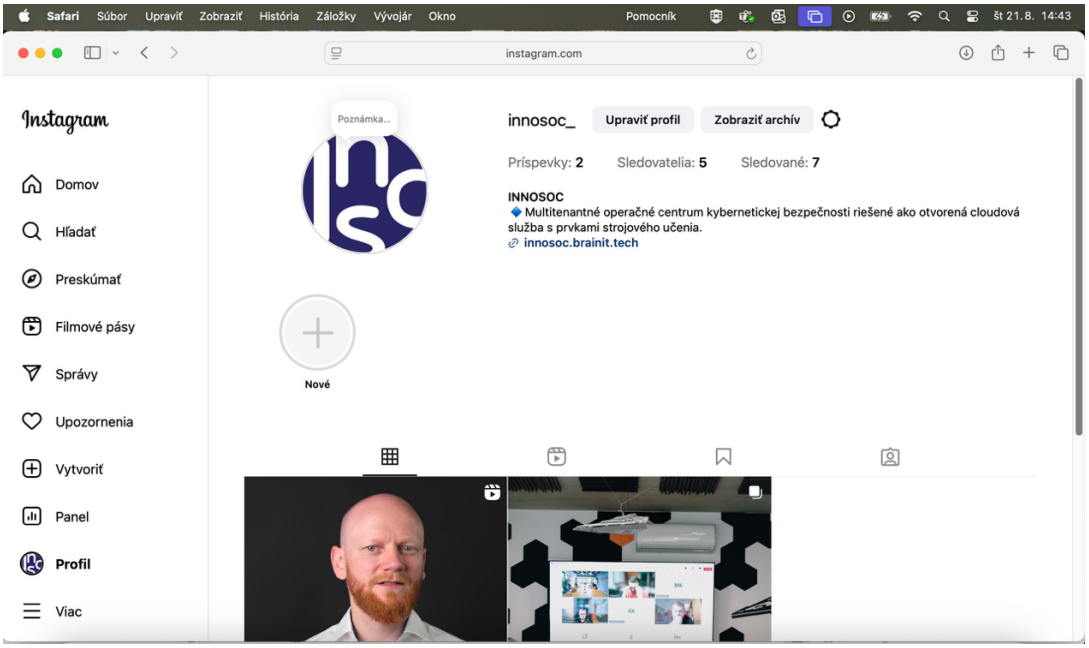
Stránka obsahuje profilovú fotografiu, titulnú fotografiu ktorá zobrazuje logá vykonávateľov. Rovnako tak sa na nej používateľ dozvie o čom projekt je, kto sú partneri projektu a cez odkaz sa dostane na webovú stránku.



Obrázok 11: LinkedIn stránka pre projekt INNOSOC, Zdroj: (BRAIN:IT, 2025)

4.2.4.2 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.



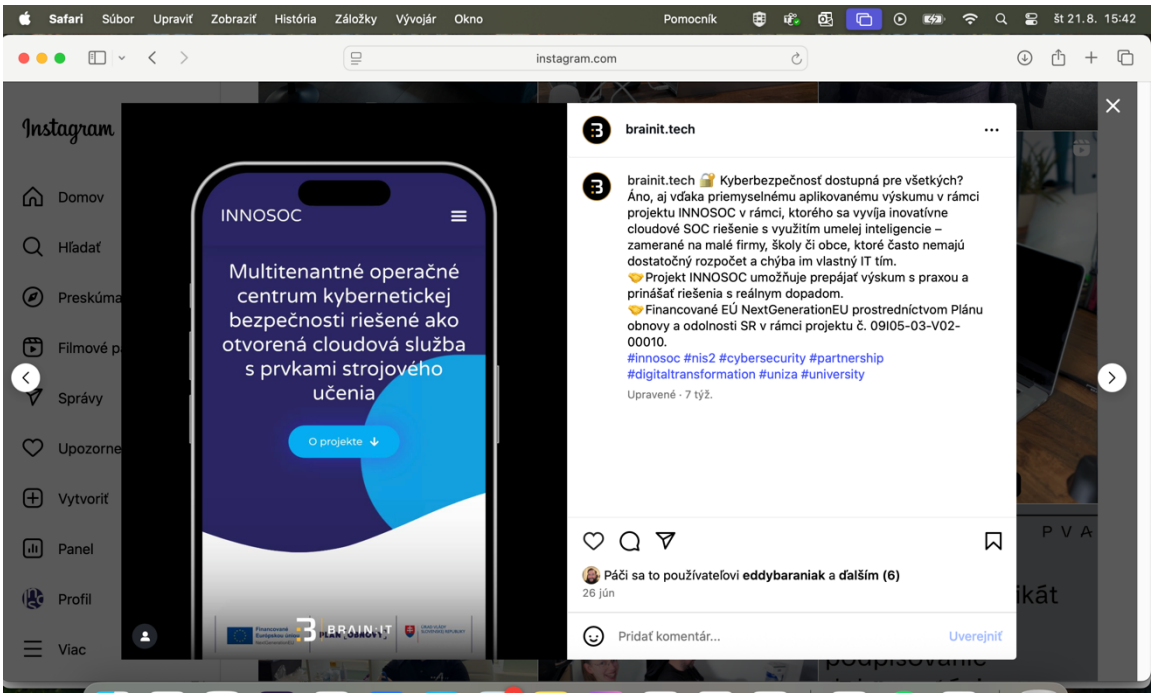
Obrázok 12: Instagramový profil INNOSOC, Zdroj: (BRAIN:IT, 2025)

4.2.4.3 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 13: Príspevok na Instagramovom účte @brain.tech, Zdroj: (BRAIN:IT, 2025)

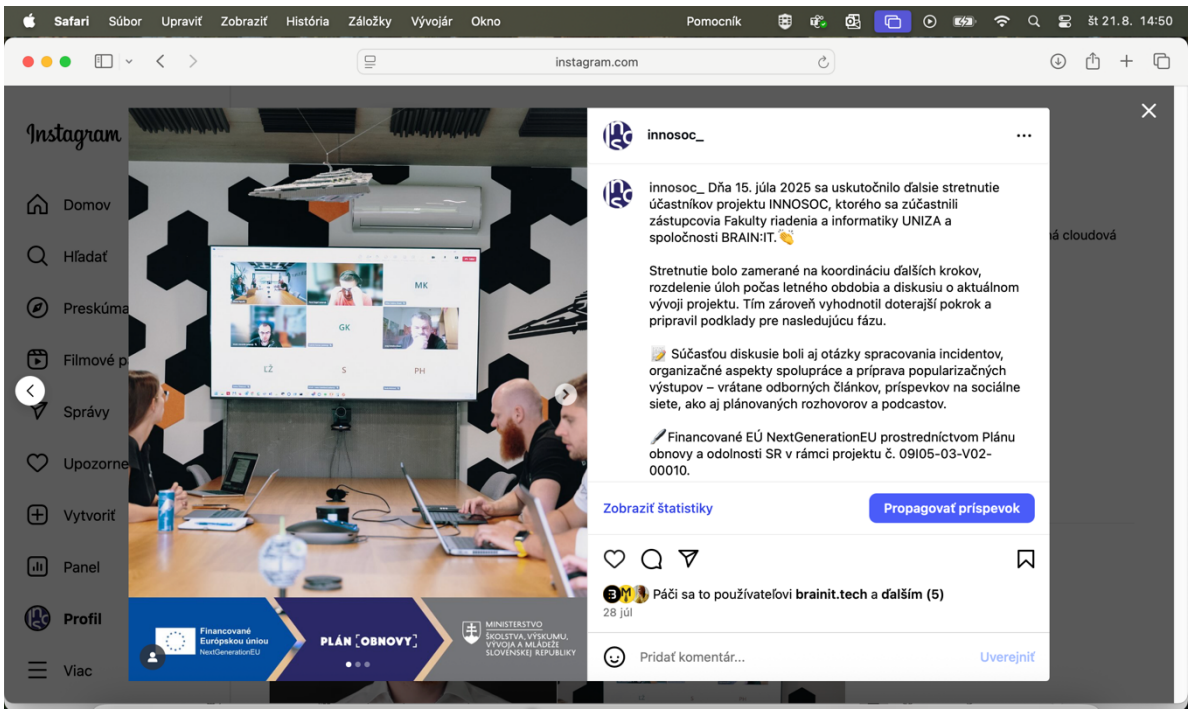
4.2.4.4 Príspevok o stretnutí partnerov 15.7.2025 na Instagrame @innosoc_

Cieľom príspevku uverejneného dňa 28. júla 2025 bolo komunikovať priebeh stretnutia partnerov projektu, spoločnosti BRAIN:IT a Fakulty riadenia a informatiky, Žilinskej univerzity v Žiline. 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.



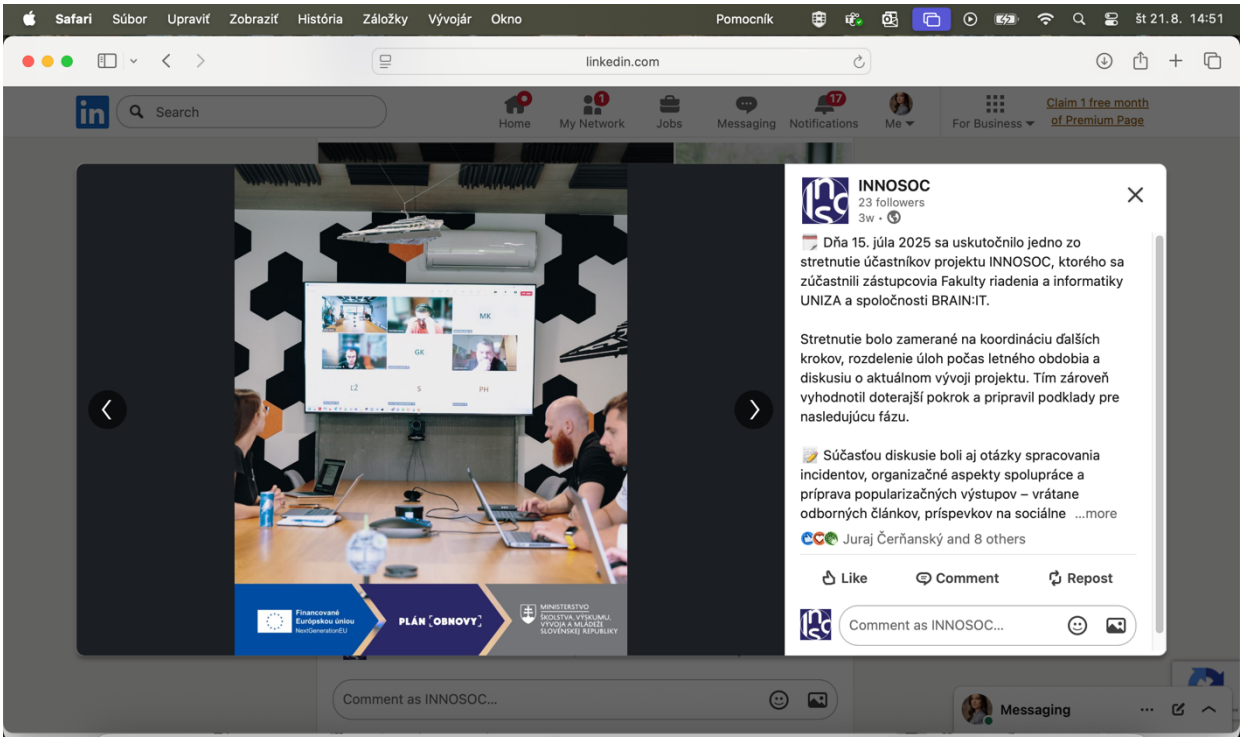
Obrázok 14: Príspevok o stretnutí partnerov 15.7.2025 na Instagrame @innosoc_, Zdroj: (BRAIN:IT, 2025)

4.2.4.5 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 Žiliny. 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 15: Príspevok o stretnutí partnerov 15.7.2025 na LinkedIne @INNOSOC, Zdroj: (BRAIN:IT, 2025)

4.2.4.6 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:

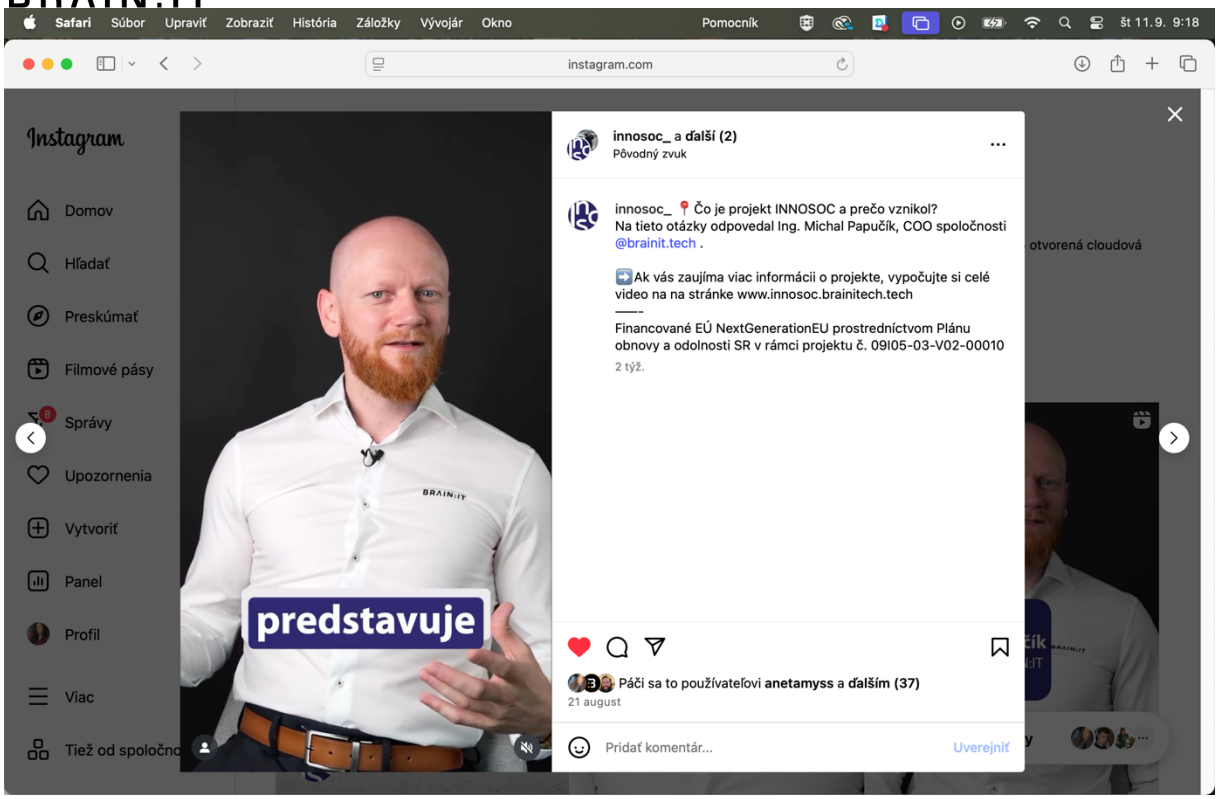
- Čo je projekt INNOSOC a prečo vznikol?
- Čo reprezentuje názov INNOSOC?

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.

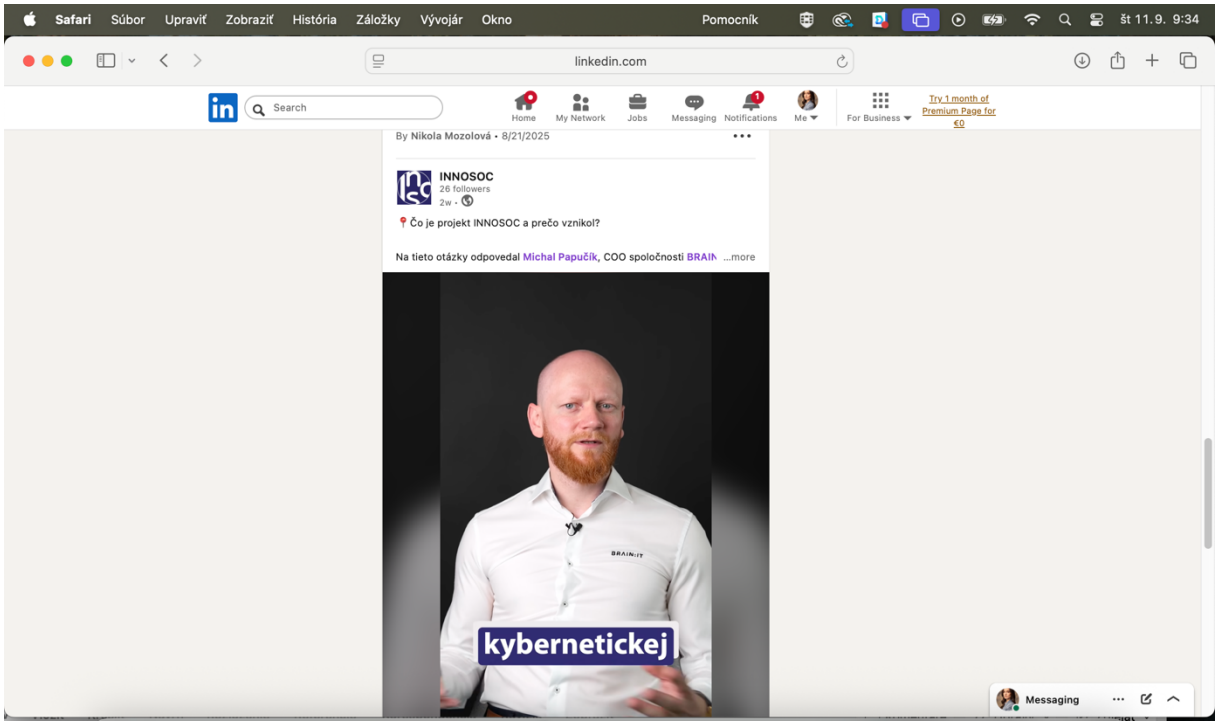
Zverejnený obsah obsahoval:

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



Obrázok 17 Príspevok vo forme krátkeho videa na LinkedIn stránke @INNOSOC z dňa 21.8.2025 , Zdroj: (BRAIN:IT, 2025)

4.2.4.7 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

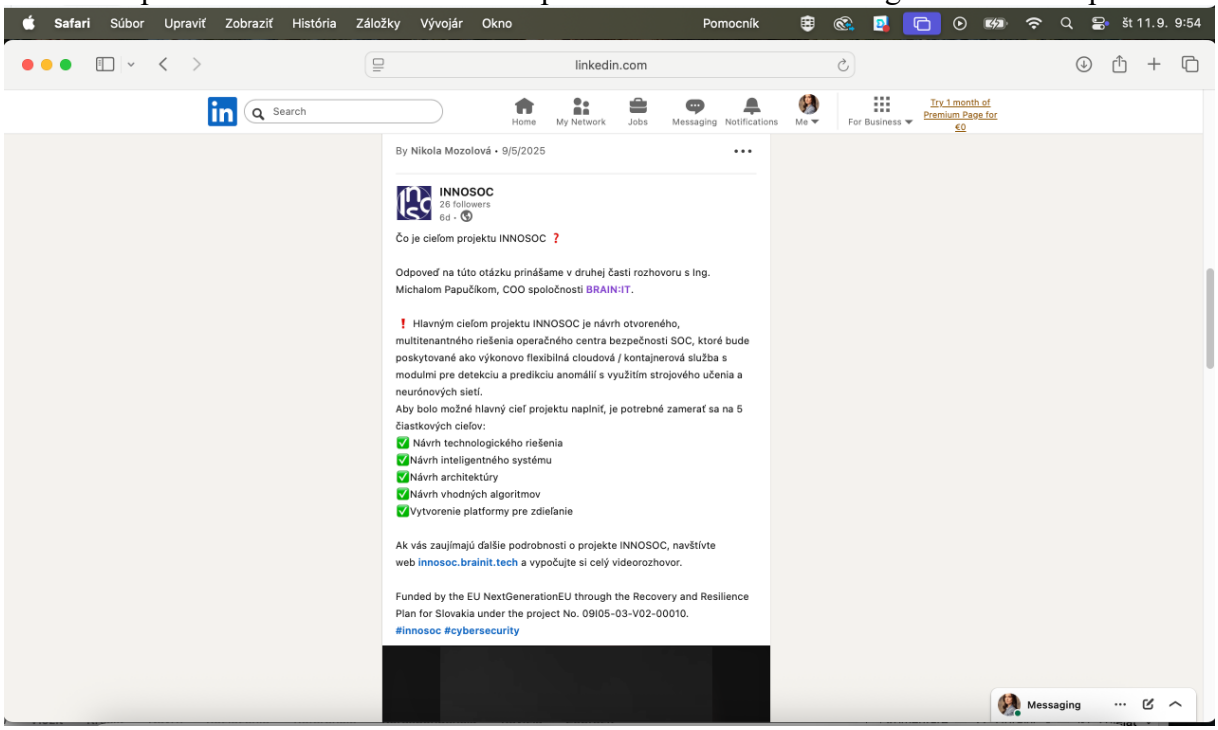
YouTube kanále @INNOSOC. Video obsahuje stručné vysvetlenie cieľa projektu. Video je spracované do formátu atraktívneho na sociálne siete tak, aby zaujalo širokú verejnosť, študentov aj mladých odborníkov.

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.

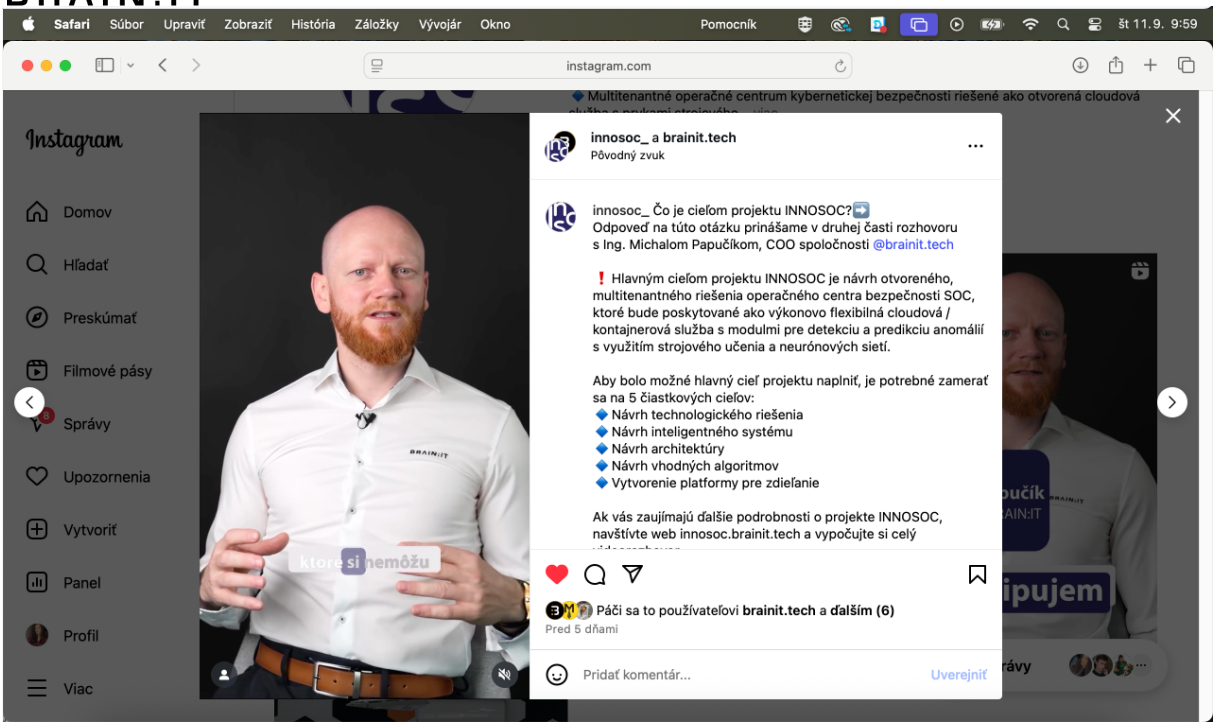
Zverejnený obsah obsahoval:

- 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.



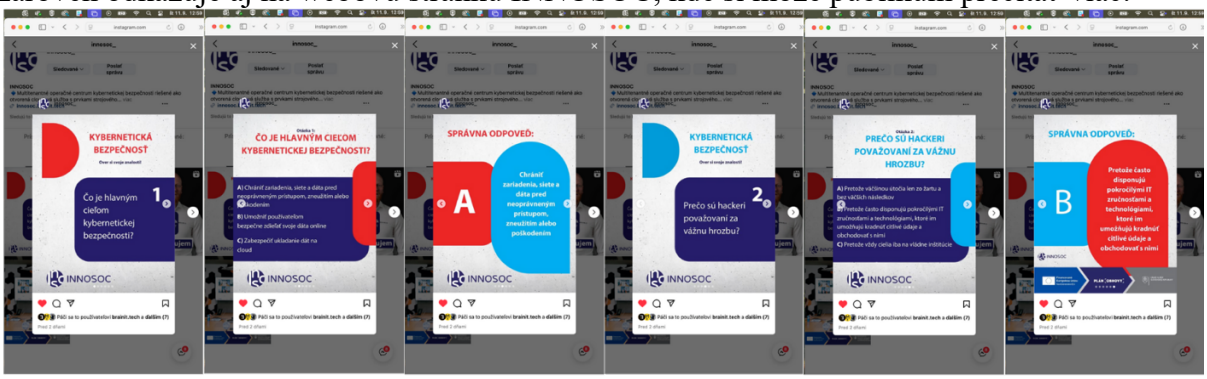
Obrázok 18 Príspevok vo forme krátkeho videa zverejnený dňa 5.9.2025 na LinkedIne @INNOSOC , Zdroj: (BRAIN:IT, 2025)



Obrázok 19 Príspevok vo forme krátkeho videa zverejnený dňa 5.9.2025 na Instagrame @innosoc_ , Zdroj: (BRAIN:IT, 2025)

4.2.4.8 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 20 Príspevok vo forme kvízu na tému kybernetická bezpečnosť zverejnený dňa 9.9.2025 na Instagrame @innosoc_, Zdroj: (BRAIN:IT, 2025)

4.2.4.9 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 21: Príspevok na instagramovom účte @innosoc_: kvíz o kybernetickeh bezpečnosti, Zdroj: (BRAIN:IT, 2025)

4.2.4.10 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 22: príspevok na instagramovom účte @innosoc_: súťaž o iPad, Zdroj: (BRAIN:IT, 2025)

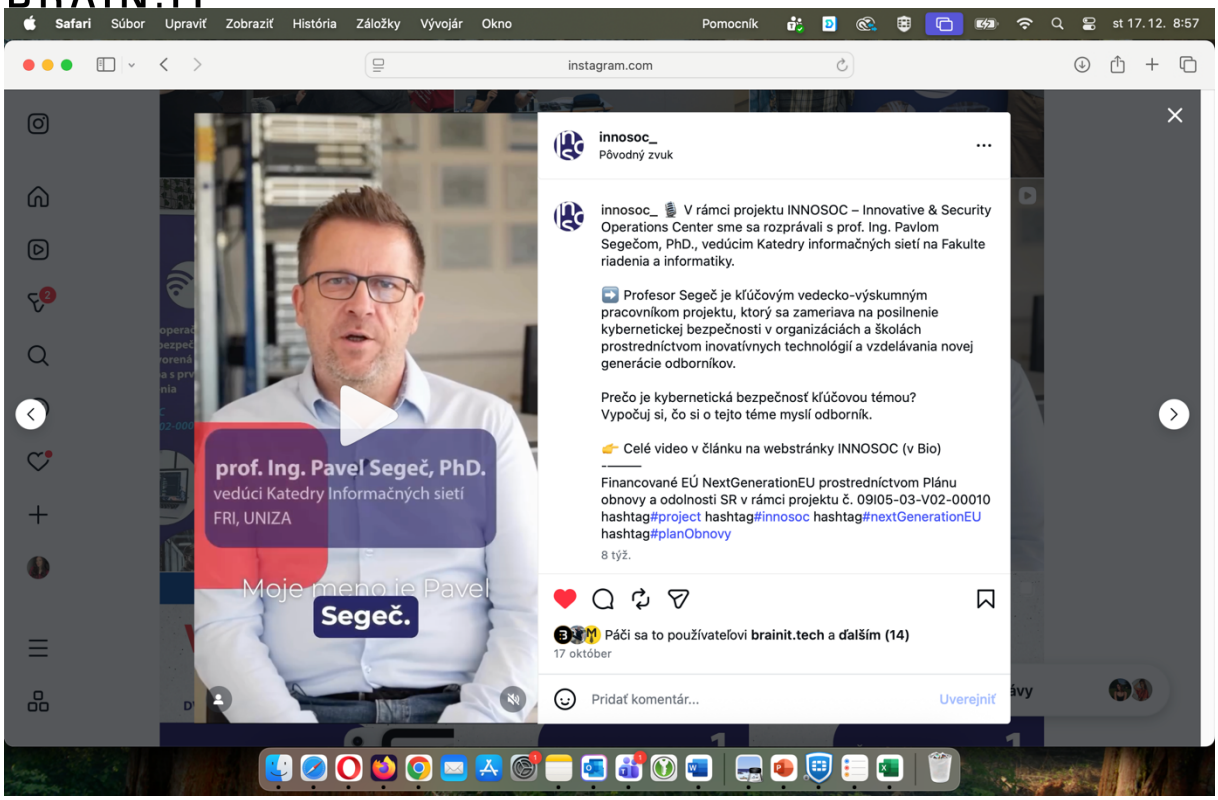
4.2.4.11 Krátke video – rozhovor s prof. Ing. Pavel Segeč, PhD.

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.

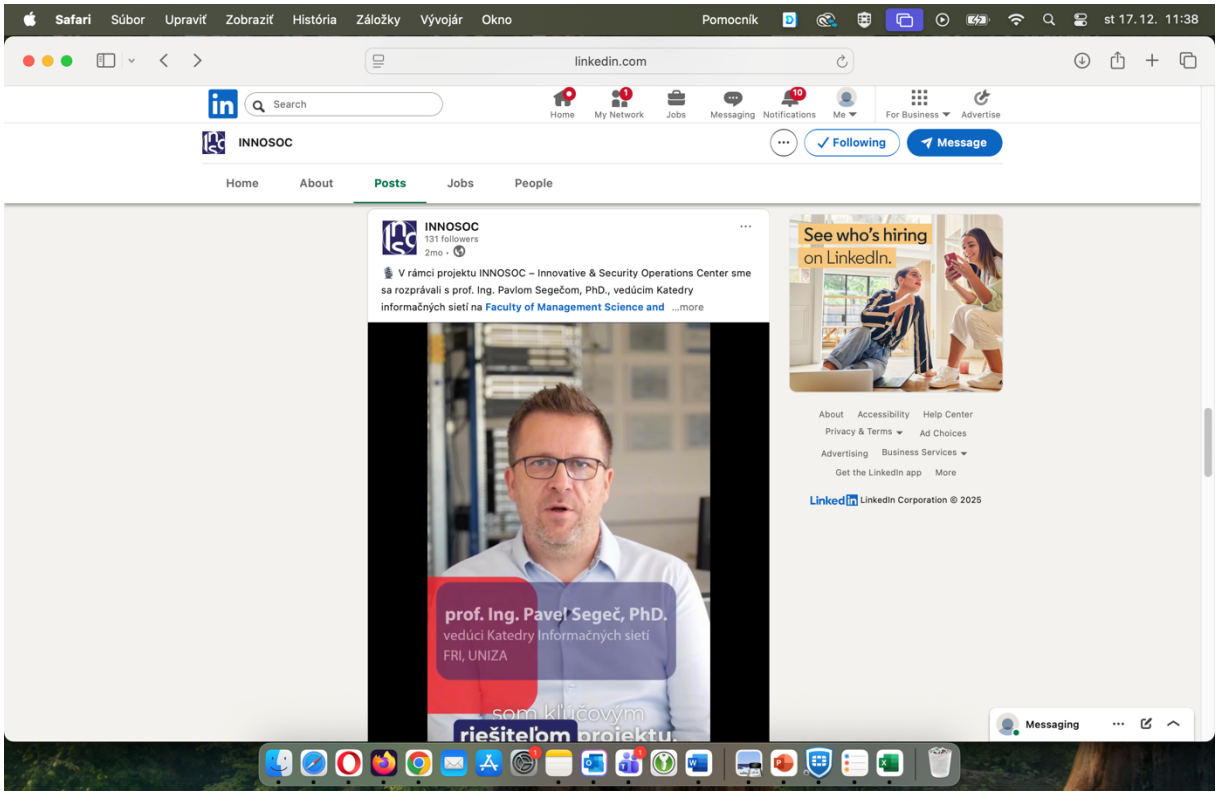
Zverejnený obsah obsahoval:

- 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 23: Krátke video na instagramovom účte @innosoc_, Zdroj: (BRAIN:IT, 2025)



Obrázok 24: krátke video na LinkedIn profile @innosoc: Rozhovor s prof. Ing. Pavel Segeč, PhD., Zdroj: (BRAIN:IT, 2025)

4.2.4.12 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.

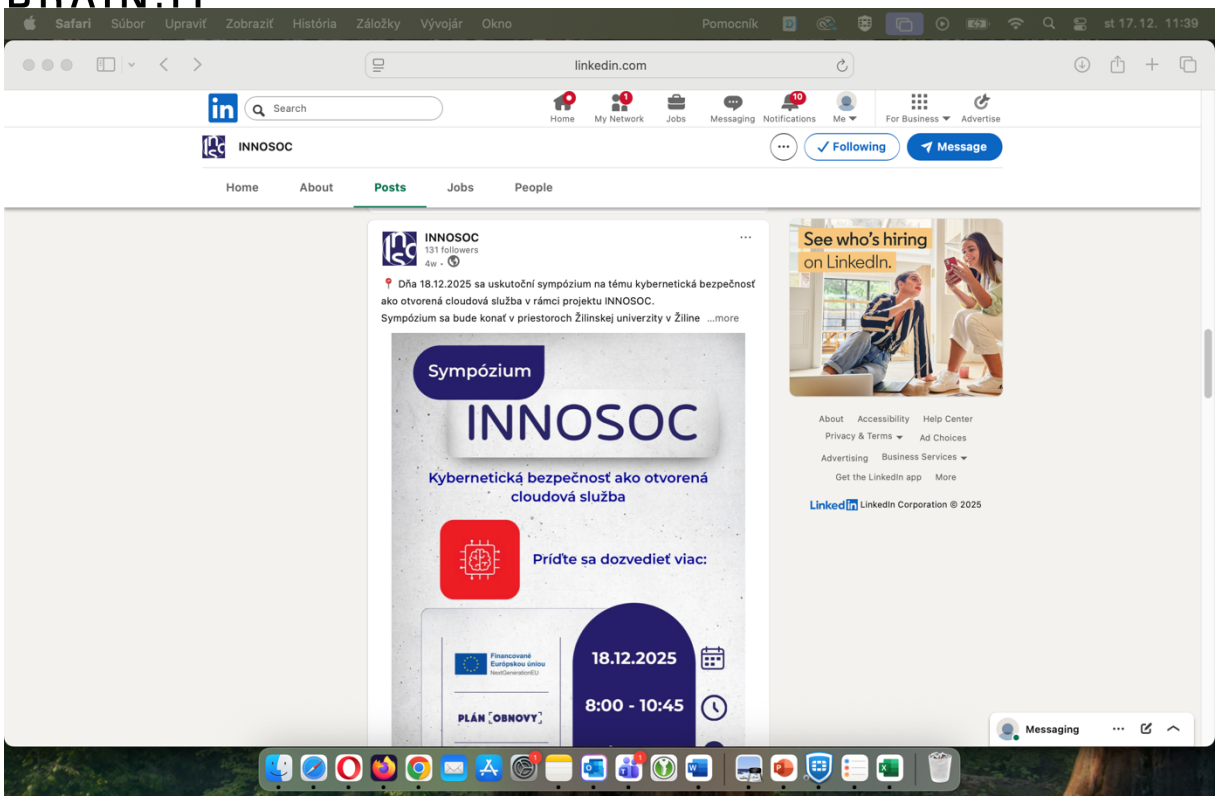
Zverejnený obsah obsahoval:

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



Obrázok 26: príspevok na LinkedIn profile @innosoc: oznam o konaní sympózia, Zdroj: (BRAIN:IT, 2025)

4.2.4.13 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.

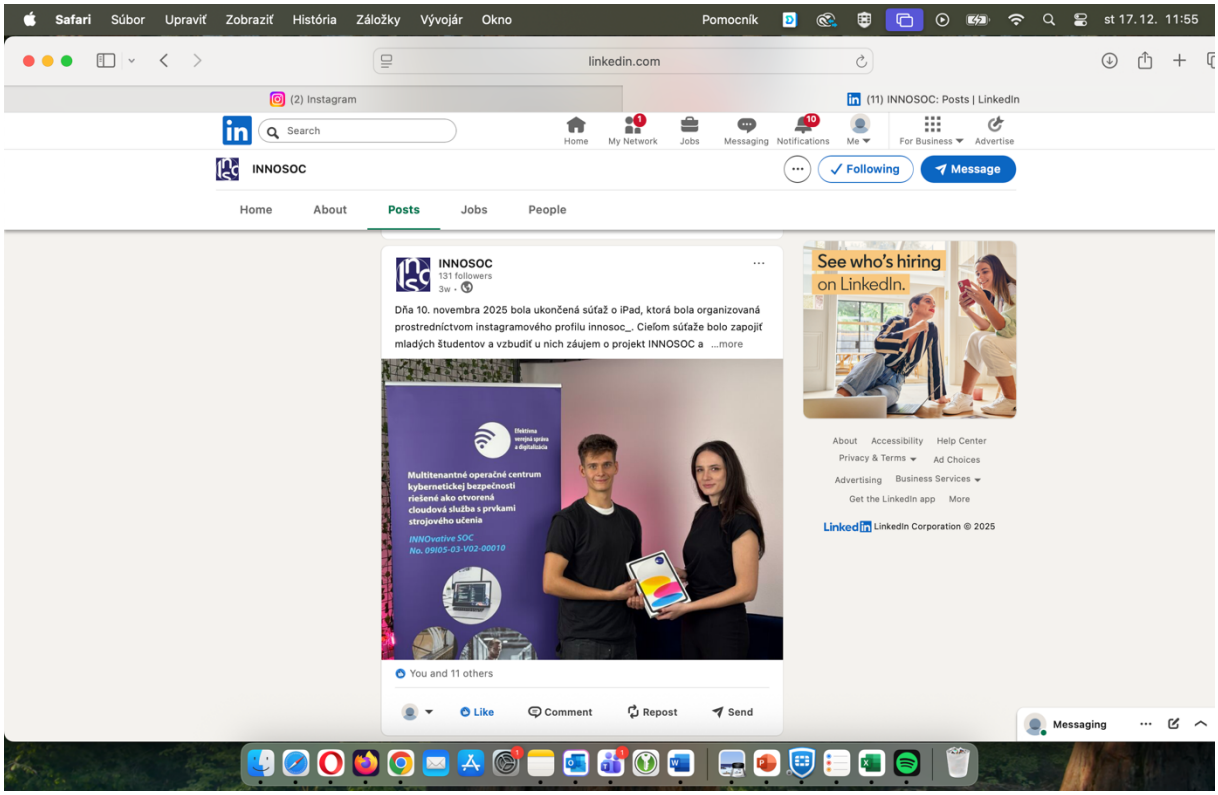
Zverejnený obsah zahŕňal:

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



Obrázok 28: prípevok na LinkedIn profile @innosoc_: odovzdávanie ceny súťaže, Zdroj: (BRAIN:IT, 2025)

4.2.4.14 Príspevok o prezentácii projektu INNOSOC na študentských raňajkách

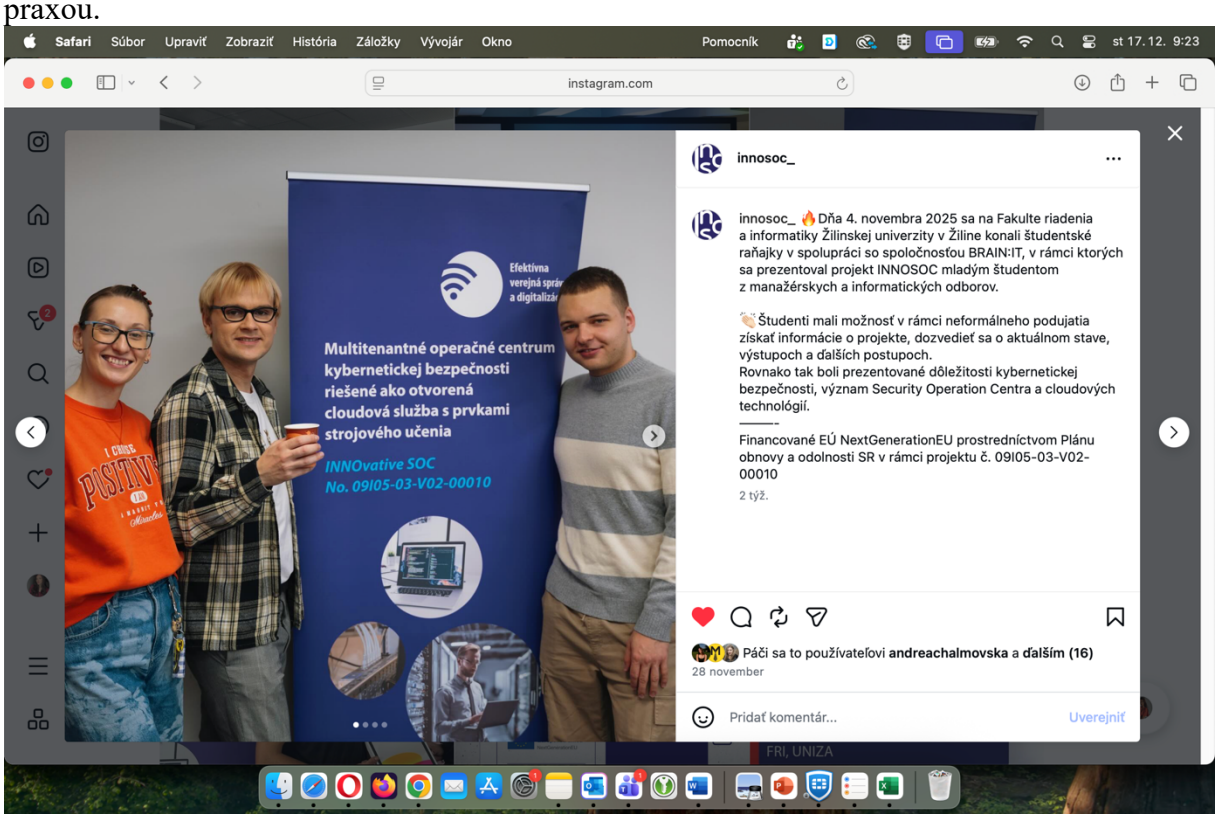
Dňa 28. novembra 2025 bol zverejnený príspevok na instagramovom profile @innosoc_ informujúci o študentských raňajkách, ktoré sa konali dňa 4. novembra 2025 na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline v spolupráci so spoločnosťou BRAIN:IT.

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

4.2.4.15 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.

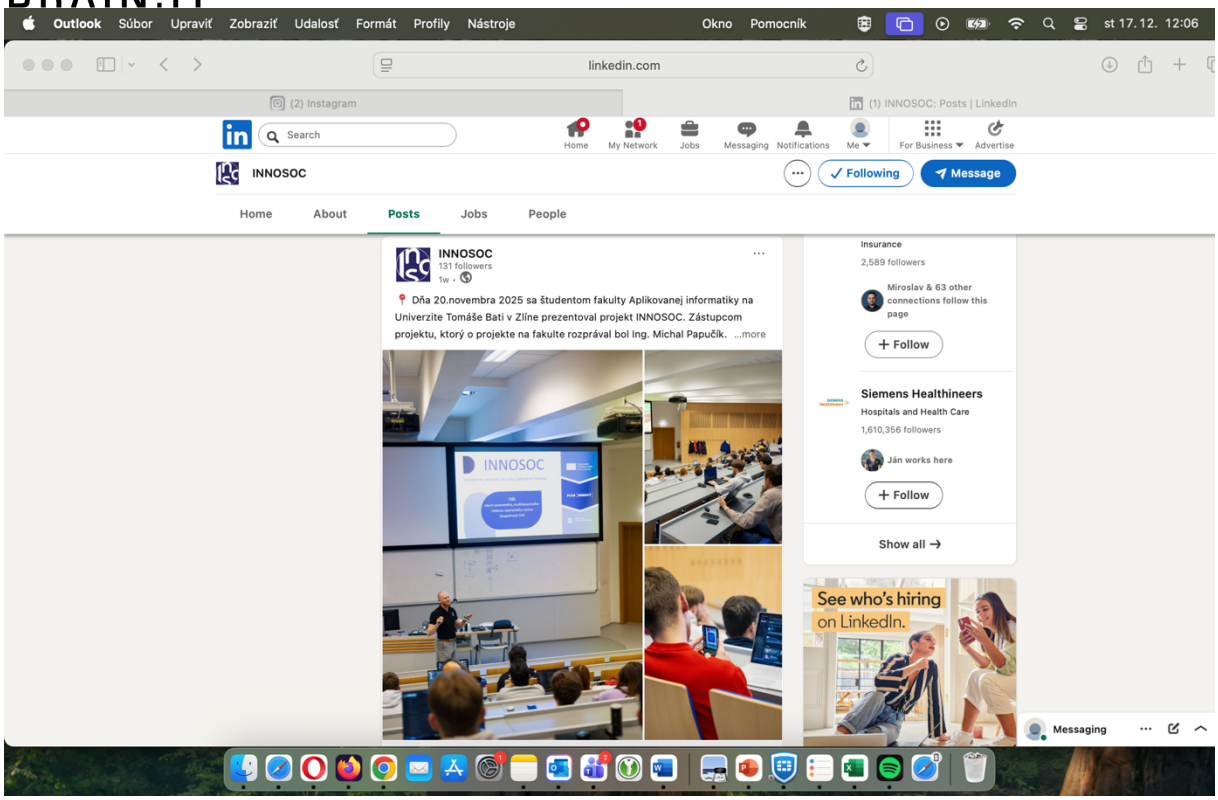
Zverejnený obsah zahŕňal:

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



Obrázok 31:príspevok na LinkedIn profile @innosoc: prezentácia na Univerzite Tomáše Báti v Zlíne, Zdroj: (BRAIN:IT, 2025)

4.2.4.16 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.

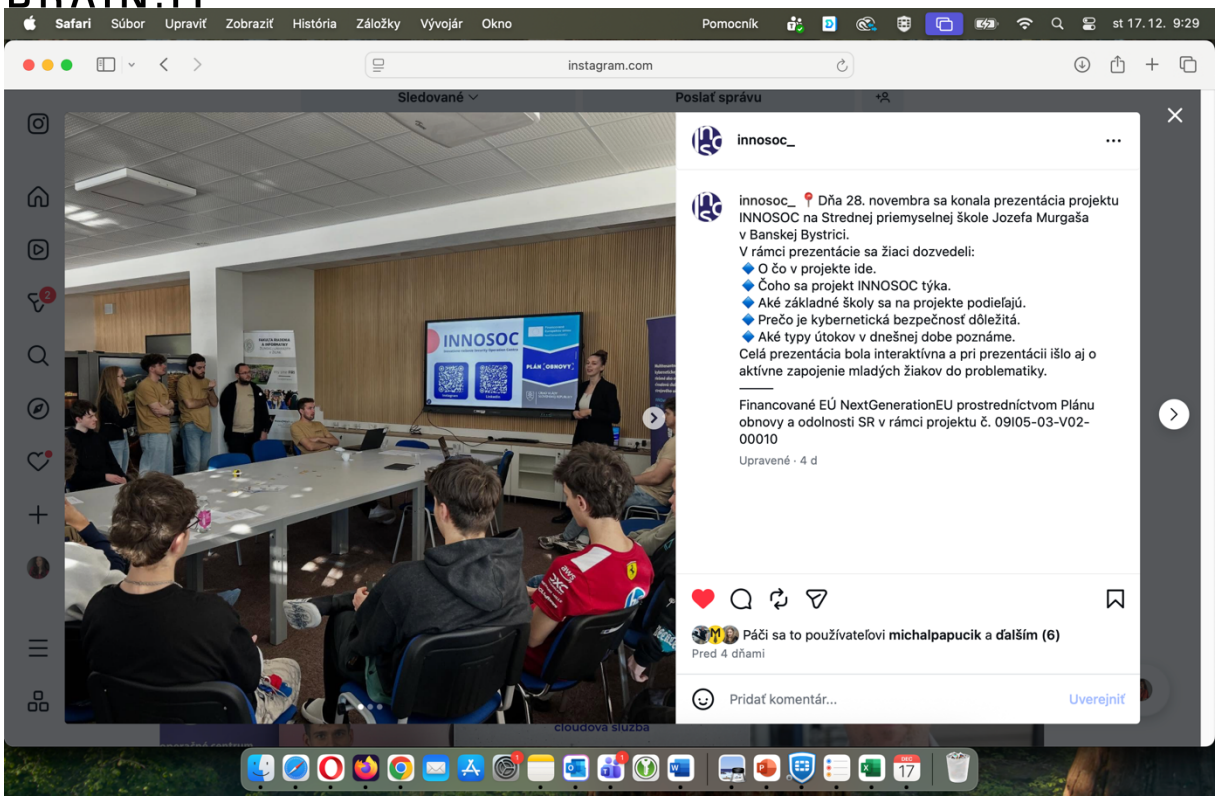
Cieľom príspevku bolo informovať verejnosť o realizácii edukačnej aktivity zameranej na zvýšenie povedomia o kybernetickej bezpečnosti medzi žiakmi stredných škôl a priblížiť im význam projektu INNOSOC v kontexte ochrany digitálneho priestoru.

Zverejnený obsah zahŕňal:

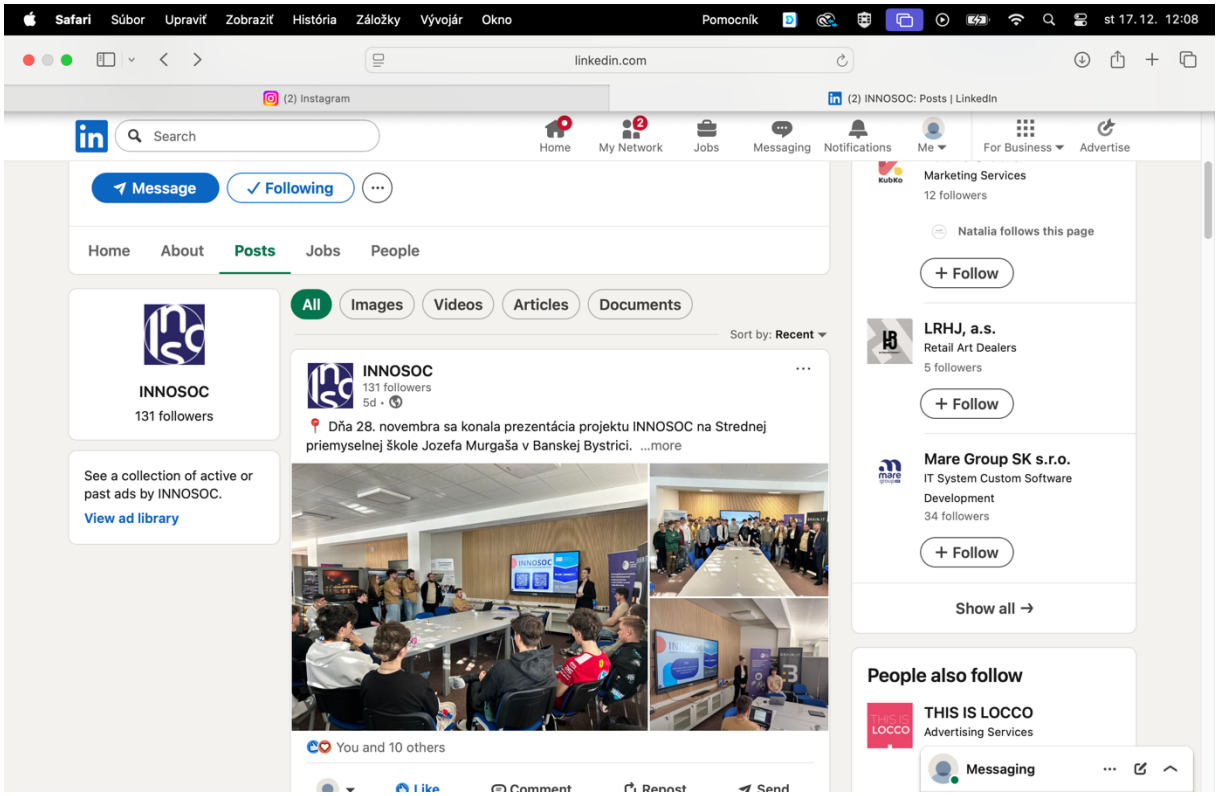
- informáciu o realizácii prezentácie projektu na strednej škole,
- predstavenie cieľov a zamerania projektu INNOSOC,
- vysvetlenie významu kybernetickej bezpečnosti a aktuálnych typov kybernetických útokov,
- prezentáciu zapojených vysokých škôl a partnerov projektu,
- interaktívny charakter prezentácie 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 32: príspevok na instagramovom profile @innosoc_: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici, Zdroj: (BRAIN:IT, 2025)



Obrázok 33: príspevok na LinkedIn profile @innosoc: prezentácia na Strednej priemyselnej škole Jozefa Murgaša v Banskej Bystrici, Zdroj: (BRAIN:IT, 2025)

4.3 Popularizačné texty

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

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

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

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

Obsahová stratégia popularizačných textov bude vychádzať z princípu postupného budovania povedomia a dôvery. Texty budú štruktúrované do tematických celkov, ktoré pokryjú základné koncepty kybernetickej bezpečnosti, predstavia inovatívne riešenia projektu INNOSOC a ukážu ich praktické využitie v reálnych scenároch. Každý text bude doplnený o vizuálne prvky ako sú schémy, infografiky alebo ilustrácie, ktoré uľahčia pochopenie zložitých technických procesov. Zároveň budú texty obsahovať interaktívne prvky ako otázky pre čitateľov, kvízy alebo odkazy na doplňujúce materiály.

Dôležitým aspektom popularizačných textov bude aj ich aktuálnosť a relevantnosť k súčasným trendom v kybernetickej bezpečnosti. Texty budú pravidelne aktualizované o nové poznatky získané počas realizácie projektu, prípadové štúdie úspešných implementácií a reflexie na aktuálne kybernetické hrozby. Tento prístup zabezpečí, že obsah zostane atraktívny a užitočný pre čitateľov dlhodobo, pričom sa webová stránka projektu stane uznávaným zdrojom informácií v oblasti kybernetickej bezpečnosti na Slovensku aj v širšom európskom kontexte.

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.

4.3.1 Realizované aktivity

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

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

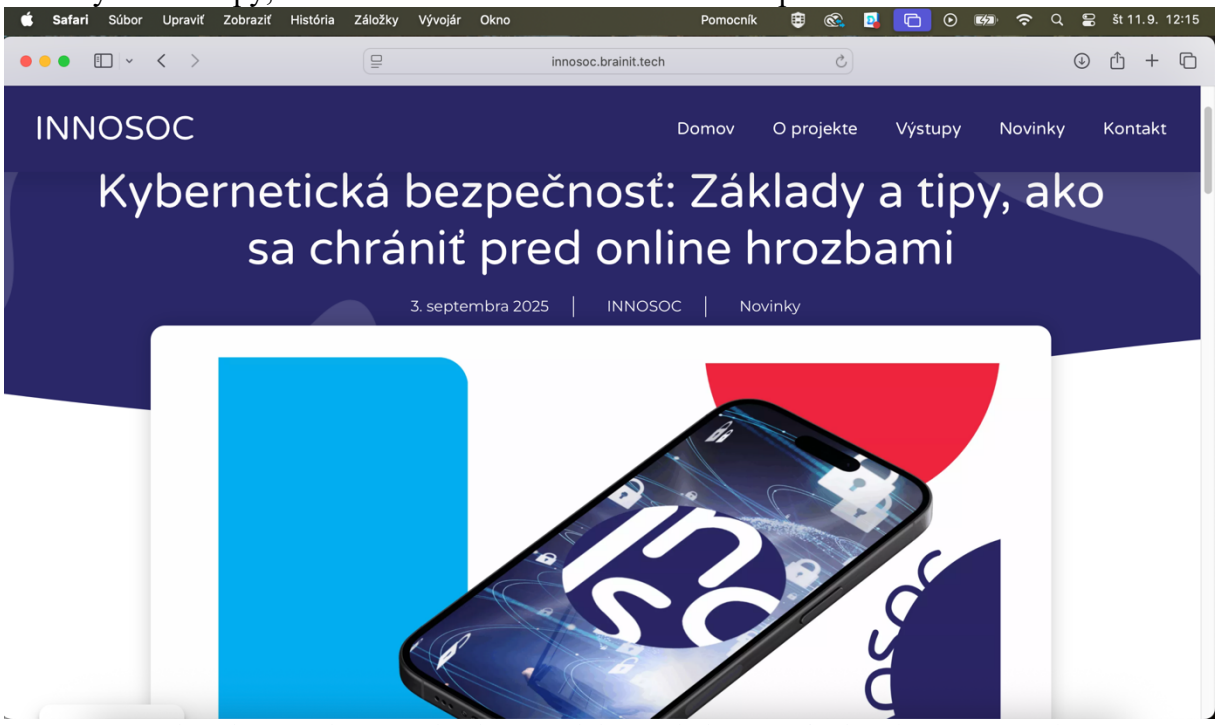
Do sekcie „Novinky“ bol 3. septembra 2025 pridaný popularizačný článok na tému Kybernetická bezpečnosť: Základy a tipy, ako sa chrániť pred online hrozbami. Cieľom článku bolo zrozumiteľnou a prístupnou formou vysvetliť základné princípy kybernetickej bezpečnosti širokej verejnosti, poukázať na aktuálne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

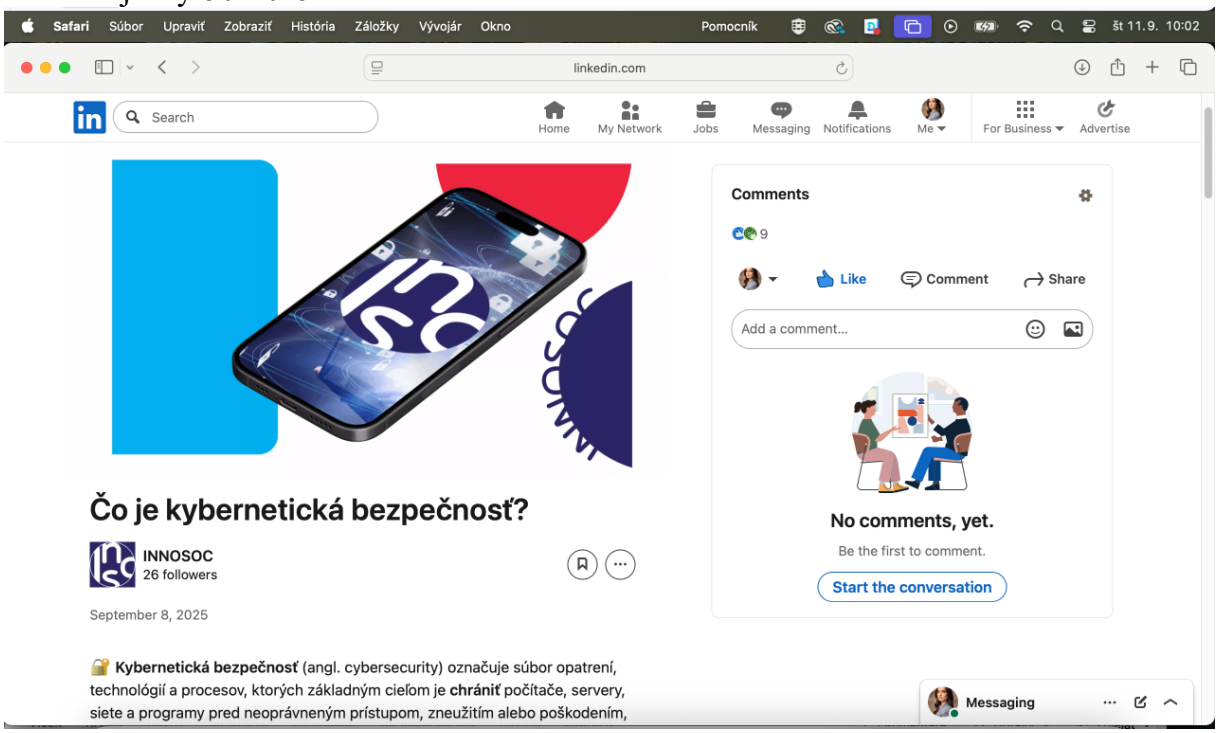
Článok slúži ako edukačný a osvetový výstup projektu, ktorého cieľom je zvýšiť povedomie o kybernetickej bezpečnosti, podporiť zodpovedné správanie používateľov v online priestore a prispieť k znižovaniu rizík spojených s digitálnymi hrozbami.

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



Obrázok 34 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 35 Popularizačný článok na tému kybernetická bezpečnosť na LinkedIn stránke @INNOSOC, Zdroj: (BRAIN:IT, 2025)

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

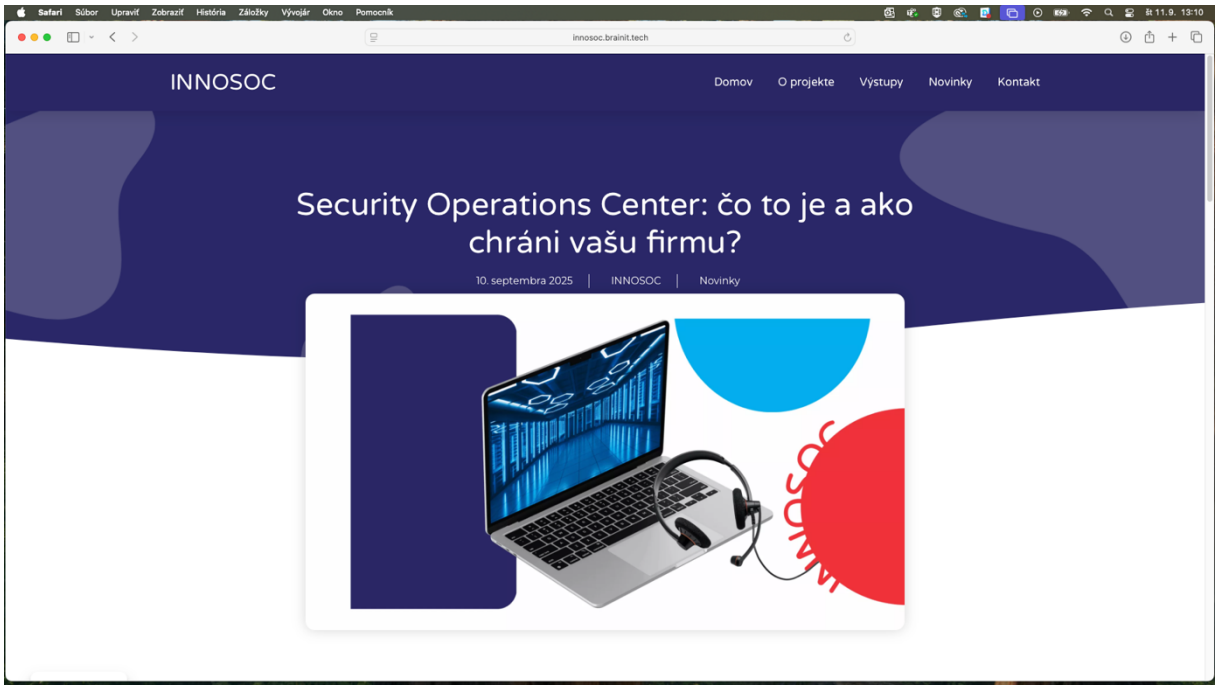
Dňa 10. septembra 2025 bol v sekcii „Novinky“ zverejnený edukačný článok na tému „Security Operations Center: čo to je a ako chráni vašu firmu?“. Cieľom článku bolo priblížiť pojem Security Operations Center ako kľúčový prvok moderného prístupu ku kybernetickej bezpečnosti a vysvetliť jeho význam pri 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 36 Popularizačný článok na tému Security Operations Center, Zdroj: (BRAIN:IT, 2025)

4.3.1.3 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.

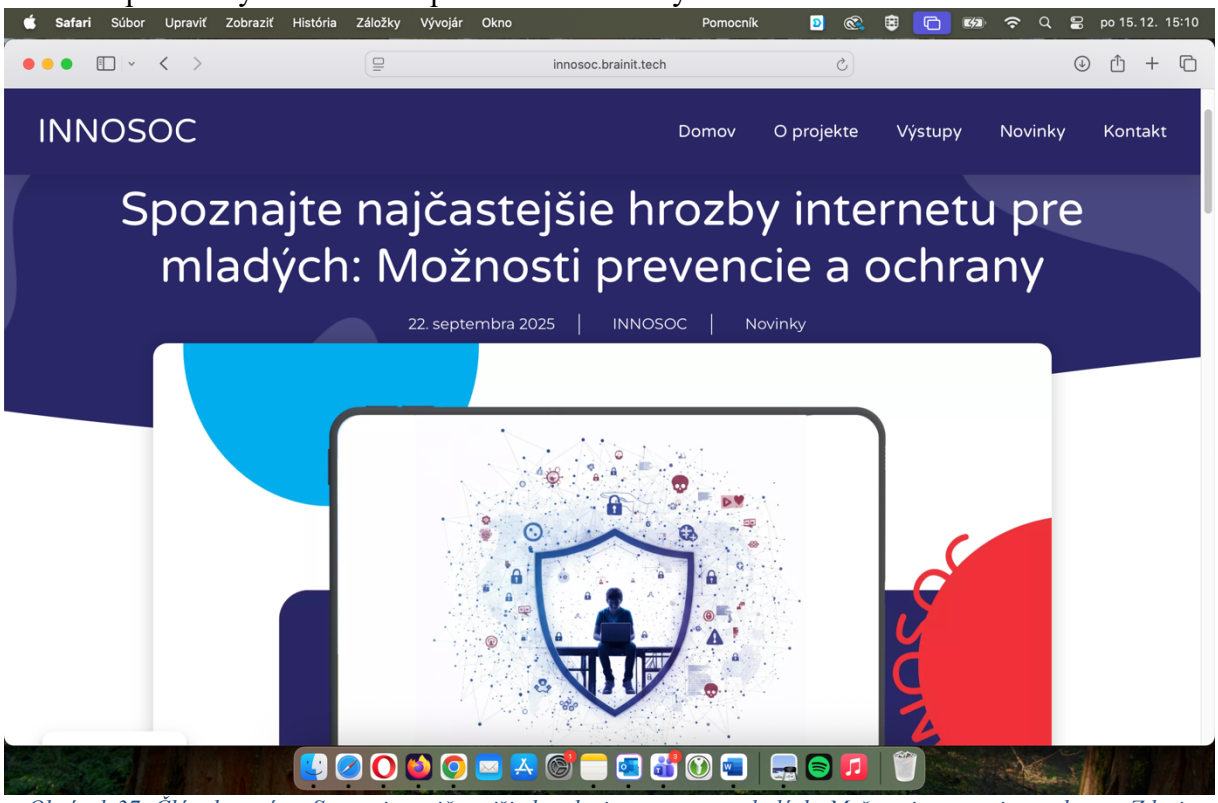
Obsah článku sa zameriava najmä na:

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

4.3.1.4 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.

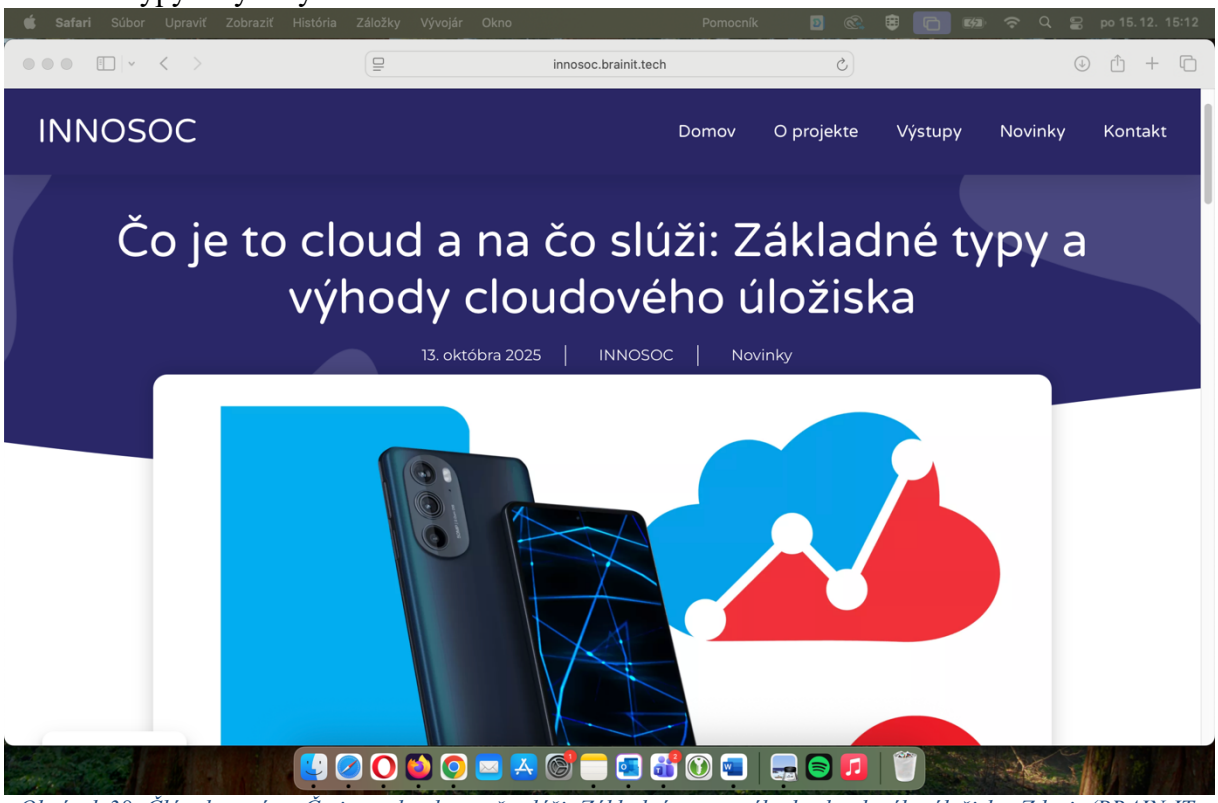
Obsah článku sa zameriava najmä na:

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

4.3.1.5 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.

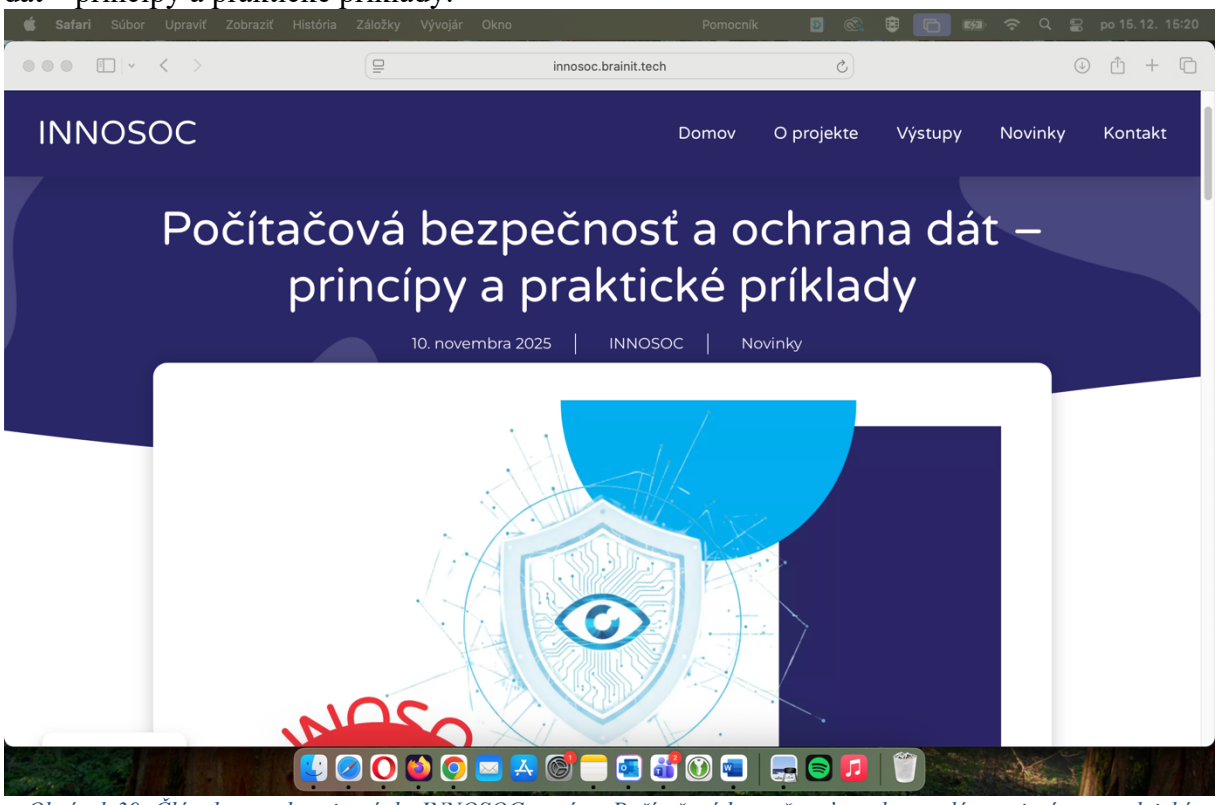
Obsah článku sa zameriava najmä na:

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

4.4 Audiovizuálny obsah

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

Ich hlavnou úlohou je dynamicky a pútavo predstaviť komplexné technické procesy a výhody SOC riešenia prostredníctvom kombinovaného audiovizuálneho obsahu, ktorý dokáže osloviť širokú škálu cieľových skupín. Budú zdieľané najmä na sociálnych sieťach a webovej stránke projektu.

Videá budú prispôsobené špecifikám jednotlivých platforiem a cieľových segmentov, pričom pre sociálne siete budú vytvorené kratšie formáty s výraznou vizuálnou stránkou, zatiaľ čo pre webovú stránku a odborné prezentácie budú pripravené detailnejšie a technicky orientované videá. Obsah bude zahŕňať vysvetlenia fungovaní SOC systémov, demonštrácie detekcie kybernetických hrozieb v reálnom čase, rozhovory s odborníkmi a testimonials od partnerov projektu.

Promo videá budú slúžiť ako kľúčový nástroj pre vzdelávanie študentov a zvyšovanie digitálnej gramotnosti širokej verejnosti, pričom budú vysvetľovať základné pojmy

kybernetickej bezpečnosti prostredníctvom praktických ukážok a vizuálnych metafor. Osobitný dôraz bude kladený na demonštráciu multitenantnej architektúry a výhod cloudových riešení, ktoré budú prezentované formou zrozumiteľných animácií a reálnych scenárov použitia.

Strategicky budú videá rozdelené do niekoľkých kategórií podľa obsahu a účelu: úvodné videá predstavujúce projekt a jeho ciele, technické tutoriály a demonštrácie pre odborníkov, edukačné videá pre študentov a laickú verejnosť, ako aj testimonials a prípadové štúdie pre potenciálnych zákazníkov. Každé video bude optimalizované pre rôzne platformy s ohľadom na ich špecifické požiadavky na formát, dĺžku a štýl obsahu.

Produkcia promo videí bude zahŕňať využitie moderných a profesionálnych produkčných nástrojov vizualizácie, animácie a postprodukcie, ktoré umožnia efektívne prezentovať abstraktné koncepty kybernetickej bezpečnosti. Videá budú obsahovať profesionálne nahovorené komentáre, kvalitné grafické prvky a hudbu, ktorá podčiarkne inovatívny charakter projektu.

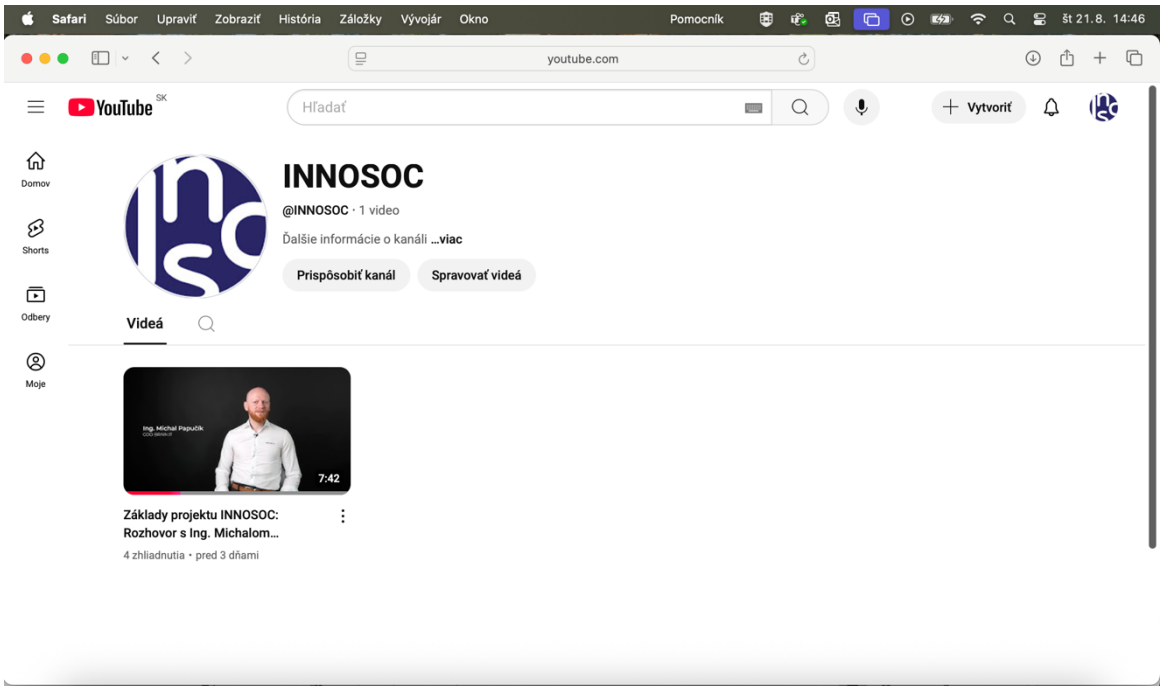
Súčasne budú videá dostupné s titulkami v slovenskom alebo anglickom jazyku, čo rozšíri ich dosah na medzinárodnú úroveň a zvýši ich využiteľnosť pre rôzne cieľové skupiny.

4.4.1 Realizované aktivity

4.4.1.1 Vytvorenie účtu na platforme YouTube

Pre publikáciu videí – najmä odborných rozhovorov, video návodov, videí z testovania 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.

Celý prepis videa sa nachádza v prílohe 15 – Rozhovor s Ing. Michalom Papučíkom.

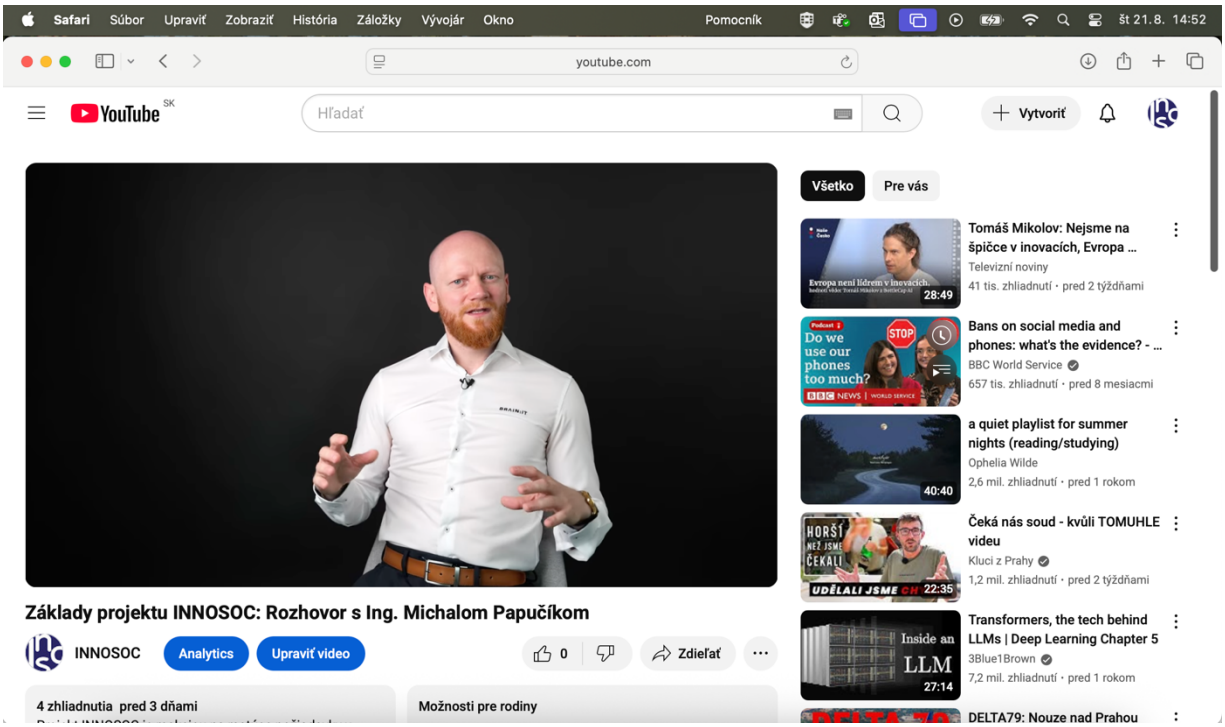


Obrázok 40: YouTube kanál @INNOSOC, Zdroj: (BRAIN:IT, 2025)

4.4.1.2 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 41: Videorozhovor s Ing. Michal Papučík, Zdroj: (BRAIN:IT, 2025)

4.4.1.2.1 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.

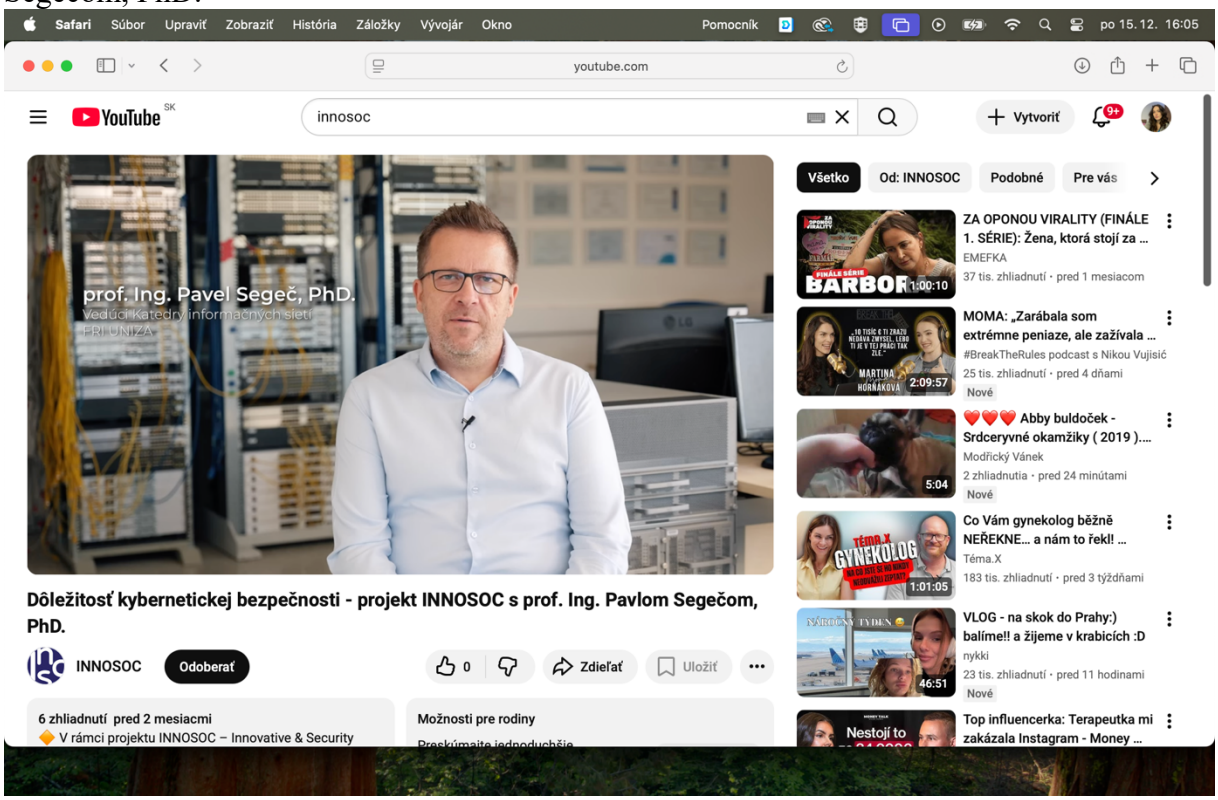
Obsah rozhovoru sa zameriava najmä na:

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

4.5 Promo materiály

Promo materiály ako brožúry, roll-upy, letáčiky a ďalšie tlačené či digitálne propagačné prvky predstavujú nenahraditeľnú súčasť komplexnej komunikačnej stratégie projektu INNOSOC. Tieto materiály slúžia ako hmatateľné nosiče informácií, ktoré umožňujú potenciálnym zákazníkom, partnerom a ostatným cieľovým skupinám získať ucelený prehľad o projekte aj mimo online prostredia.

Ich hlavnou úlohou je vizuálne atraktívnym a profesionálnym spôsobom predstaviť kľúčové výhody SOC riešenia, technické špecifikácie a obchodný potenciál projektu pri osobných stretnutiach, konferenciách a obchodných rokovaniach.

Dizajn a obsah promo materiálov budú striktne diferencované podľa jednotlivých cieľových segmentov a účelu použitia. Pre odbornú verejnosť budú pripravené technicky orientované brožúry s detailnými architektúrnymi schémami a výskumnými výstupmi.

Pre potenciálnych zákazníkov z radov malých a stredných podnikov budú vytvorené obchodne zamerané letáčiky zdôrazňujúce cost-benefit analýzu a praktické prínosy SOCaaS riešenia. Študentom budú určené farebné a vizuálne pútavé materiály s prvkami gamifikácie a motivačnými prvkami pre ich budúcu kariéru v oblasti kybernetickej bezpečnosti.

Osobitne dôležitú úlohu budú hrať promo materiály v rámci direct sales aktivít zameraných na potenciálnych zákazníkov. Roll-upy a prezentačné brožúry budú nevyhnutným nástrojom pri obchodných stretnutiach, kde budú slúžiť ako vizuálna podpora pre sales prezentácie.

Materiály budú k dispozícii na odborných konferenciách, univerzitných podujatiach a v priestoroch partnerských organizácií.

Digitálne verzie budú dostupné na webovej stránke projektu na stiahnutie, pričom budú optimalizované pre rôzne zariadenia a formáty. Každý materiál bude obsahovať QR kódy prepájajúce na webovú stránku a špecifické landing pages pre meranie konverzií a efektívnosti jednotlivých kampaní.

4.5.1 Realizované aktivity

4.5.1.1 Informačný leták INNOSOC

Pre účely prezentovania a rozširovania povedomia o projekte bol vytvorený informačný leták, ktorý komunikuje základe informácie o projekte, ako je jeho cieľ, čiastkové ciele a problematiku, na ktorú výskumný projekt INNOSOC reaguje.



Obrázok 43: Informačný poster projektu INNOSOC, Zdroj:

4.5.1.2 *Informačný poster pre sympózium*

Pre komunikáciu organizácie sympózia INNOSOC s témou „Možnosti umelej inteligencie v kybernetickej bezpečnosti“, ktoré sa bude konať 18.decembra 2025 v priestoroch Žilinskej univerzity v Žiline bol vytvorený poster. Informačný poster komunikuje dátum, čas, miesto a tému sympózia.



Obrázok 44: Informačný poster o konaní sympózia INNOSOC, Zdroj:

5 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). *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

6 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 Brainit-y riešime v rámci nášho vývoja v projekte INNOSOC.