Cluster Kybernetickej Bezpečnosti

Stratégia rozvoja klastrovej organizácie

Pre obdobie 2020-2023

Ing. Ján Lichvár

18.11.2020

Obsah

1 Digitalizácia v Slovenskej republike 4
2 Súčasný stav odvetvia kybernetickej bezpečnosti 6
2.1 SWOT analýza odvetvia kybernetickej bezpečnosti v regióne Žilinského samosprávneho kraja s presahom na územie Slovenskej republiky 7
2.2 Súčasný stav a analýza Clustra Kybernetickej Bezpečnosti 8
2.2.1 Vznik 8
2.2.2 Členovia 8
2.2.3 Predmet činnosti 9
2.2.4 Štruktúra, riadenie a financovanie činnosti 10
2.2.5 Predmet činnosti 11
2.2.6 Marketing 12
2.3 SWOT analýza Clustra Kybernetickej Bezpečnosti 13
3 Poslanie, vízia, stanovenie cieľov a priorít 14
3.1 Poslanie a vízia 14
3.2 Ciele 18
3.2.1 Vytvorenie Centra excelentnosti kybernetickej bezpečnosti 18
3.2.2 Vzdelávanie členov, nadviazanie spolupráce s novými partnermi, internacionalizácia 19
3.2.3 Vzdelávacie, odborné, informačné a osvetové podujatia 20
3.3 Súlad cieľov Clustra Kybernetickej Bezpečnosti so stratégiou výskumu a inovácií pre inteligentnú špecializáciu Slovenskej republiky (RIS 3 SK) 22
4 Akčné plány 24
4.1 Akčný plán 1 - vytvorenie Centra excelentnosti kybernetickej bezpečnosti ..24
4.1.1 Priebeh 24
4.1.2 Časový harmonogram 25
4.1.3 Financovanie 25
4.1.4 Personálne zabezpečenie 25

4.2 Akčný plán 2 - vzdelávanie členov a nadviazanie spolupráce, internacionalizácia 27
4.2.1 Priebeh 27
4.2.2 Časový harmonogram 31
4.2.3 Financovanie 31
4.2.4 Personálne zabezpečenie 31
4.3 Akčný plán 3 - vzdelávacie, odborné, informačné a osvetové podujatia 32
4.3.1 Priebeh 32
4.3.2 Časový harmonogram 33
4.3.3 Financovanie 33
4.3.4 Personálne zabezpečenie 33
5 Kontrolný mechanizmus 34
6 Záver 36

1 Digitalizácia v Slovenskej republike

Potreba vytvorenia stratégie pre našu klastrovú organizáciu na nadchádzajúce obdobie je logickým krokom nadväzujúcim na založenie organizácie samotnej a reakciou na dianie v oblasti našej činnosti v našom regióne, v rámci Slovenskej republiky, Európskej Únie i celosvetovo. Digitalizácia sveta je jedným z dominantných trendov súčasnosti, a je vhodné a ba priam nutné na tento trend reagovať. Digitalizácia našej krajiny má svoje osobitosti a úskalia, ktoré tento nevyhnutný proces spomaľujú a sťažujú. Poslaním našej organizácie je pôsobiť smerom k dosiahnutiu minimálne európskej úrovne v oblasti našej činnosti.

Proces zmeny k digitalizácii je žiadúci pre všetky odvetvia slovenského hospodárstva, verejnú správu a samosprávy. Je možné predvídať, že ťahúňmi hospodárstva sa stanú práve subjekty, ktoré budú v krátkej dobe inovovať svoje procesy, zrealizujú ich digitalizáciu v najširšej možnej miere, a budú pripravené na online prostredie. Digitalizácia s určitosťou pomôže takýmto subjektom k budovaniu silného a stabilného miesta na slovenskom trhu, ale aj v zahraničí, s možnosťou rozvoja spolupráce so zahraničnými partnermi.

Subjekty (vrátane klastrových organizácií) s jasne definovanou stratégiou prechodu do online prostredia považujeme za avantgardu digitalizácie zasluhujúcu si podporu a pozornosť (aj zo strany štátu a verejných rozvojových schém), nakoľko môžu slúžiť ako pozitívny príklad pre subjekty, ktoré z rôznych dôvodov ekonomické a personálne predpoklady a stratégiu pre prechod do on-line prostredia nemajú.

Ponuka podpory, zdrojov, odbornosti, zavedených noriem, podnieti aj menších hráčov na trhu, ktorí v súčasnosti nevedia ako postupovať v rýchlo meniacom sa v digitálnom svete, aby vstúpili do procesu prechodu na digitálny trh. Nevyhnutnosť komunikácie a rozvoj spolupráce medzi jednotlivými hospodárskymi odvetviami, podnikateľskou sférou, klastrovými organizáciami, štátnou správou a samosprávami je jednou z nosných tém činnosti našej klastrovej organizácie. Prostredníctvom klastrových organizácií pôsobiacich v rôznych úrovniach geograficky a odvetvovo diverzifikovaných sa šíria informácie a pozitívne príklady z praxe medzinárodných klastrov.

Digitalizácia spoločnosti je založená na spracúvaní informácií (dát). Neoddeliteľnou súčasťou procesu digitalizácie je dosiahnutie a udržanie stavu (kybernetickej) bezpečnosti, ochranou dát vo všetkých úrovniach spoločnosti. Pre dosiahnutie stavu kybernetickej bezpečnosti je potrebné disponovať kvalifikovanou pracovnou silou s vysokou úrovňou digitálnych zručností. Situácia v tejto oblasti vzdelávania nie je ideálna a zasluhuje si podľa nášho presvedčenia podstatne väčšiu mieru pozornosti zo strany spoločnosti (štátu).

Digitalizácia spoločnosti je nezvratným procesom. Jej výsledkom je liberalizácia trhu s jej inherentnými pozitívami a negatívami. Predpokladom pre využitie potenciálu digitalizácie je vzdelávaním podporovať inovácie a prinášať dobré príklady zo zahraničia. Cieľom je potom dosiahnuť uplatnenie slovenských subjektov na domácom ako aj medzinárodnom trhu.

2 Súčasný stav odvetvia kybernetickej bezpečnosti

Odvetvie kybernetickej bezpečnosti v Slovenskej republike celkovo, aj regionálne je bezpochyby v začiatkoch budovania všeobecnej informovanosti, zavádzania procesných postupov a právnej úpravy a technológií.

Digitalizácia spoločnosti si vyžaduje ochranu pred hrozbami, elimináciu rizika a zavádzanie inovatívnych metód, postupov a procesov pre zabezpečenie kybernetickej bezpečnosti digitálneho prostredia (Internet of Things - IoT, Industry 4.0, výrobné technológie – ICS / OT /SCADA).

Hlavnou témou je zavádzanie nástrojov monitoringu digitálneho priestoru, ktoré umožňuje vytvoriť základ pre uplatnenie inovatívnych metód a postupov (strojové učenie, umelá inteligencia, korelačné analýzy, behaviorálne analýzy, atď.) a tak výrazne obmedziť pravdepodobnosť vzniku kybernetických incidentov a eliminovať riziko možných hrozieb pre digitálne prostredie.

2.1 SWOT analýza odvetvia kybernetickej bezpečnosti v regióne Žilinského samosprávneho kraja s presahom na územie Slovenskej republiky

STRENGHTS / Silné stránky	**WEAKNESSES / Slabé stránky**
• Člen Clustra Kybernetickej Bezpečnosti, spoločnosť AXENTA s.r.o. so sídlom na území Žilinského kraja, dosahuje vysokú mieru expertízy v oblasti monitoringu kybernetickej bezpečnosti s akreditáciou na CSIRT Cyber Security Incident Response Team v organizácii Trusted Introducer, ktorá združuje jednotky CSIRT po celom svete	• Nedostatok odborných ľudských zdrojov. • Nízka informovanosť o možných hrozbách a rizikách kybernetických útokov. • Absentujúci proces vzdelávania (stredoškolského i vysokoškolského) v tomto odvetví.
OPPORTUNITIES / Príležitosti	**THREATS / Hrozby**
• Potenciál spoločností so schopnosťou rýchlej adaptácie sa zo služieb v oblasti informačných technológií na služby v oblasti kybernetickej bezpečnosti. • Duálne vzdelávanie na odborných stredných školách v spolupráci s prevádzkovateľmi základnej služby. • Kooperácia škôl a klastrovej organizácie s medzinárodnými partnermi. • Zvyšovanie povedomia verejnej, súkromnej sféry formou workshopov, konferencií a webinárov.	• Podceňovanie hrozieb kybernetických útokov. • Nedostatok finančných zdrojov. • Nedostatok personálnych zdrojov. • Ekonomické dopady pandémie spôsobené ochorením COVID – 19. • Medzinárodná ekonomická nestabilita. • Neustále prebiehajúce (cyber) útoky na infraštruktúru v Slovenskej republike.

2.2 Súčasný stav a analýza Clustra Kybernetickej Bezpečnosti

2.2.1 *Vznik*

Podnetom pre vznik Clustra Kybernetickej Bezpečnosti bola absencia profesijného združenia v oblasti kybernetickej bezpečnosti, ktoré by mohlo byť partnerom pre ústredné orgány štátu, a ktoré by napomáhalo k dosiahnutiu spoločnej synergie v tejto oblasti. Jednou z priorít klastra je zlepšiť konkurencieschopnosť a produktivitu členov klastra formou vzájomnej spolupráce a prispievať k zavádzaniu inovácií v Slovenskej republike. Združenie v roku 2018 založili spoločnosti: AXENTA s.r.o., hbr advokáti s.r.o., a Salutis Systems, a.s. . Postupne sa k združeniu pridali ďalší členovia, v roku 2020 má Cluster Kybernetickej Bezpečnosti šestnásť členov.

2.2.2 *Členovia*

- Aliga, s.r.o. – poskytovateľ komplexných riešení v oblasti sieťovej infraštruktúry a jej bezpečnosti.
- AXENTA s.r.o – spoločnosť zaoberajúca sa poskytovaním riešení v oblasti monitoringu kybernetickej bezpečnosti.
- BELL TEC, a. s. – spoločnosť v oblasti vývoja a dodávky bezpečnostných a komunikačných aplikácií.
- Consulting & Education Partners, s.r.o. - spoločnosť pôsobiaca v oblasti vzdelávania, odborného poradenstva a verejného obstarávania.
- Grant Thornton Advisory s.r.o. – poskytovateľ služieb v oblasti manažérskeho a transakčného poradenstva a oceňovania.
- hbr advokáti s.r.o. – advokátska kancelária zameraná na poskytovanie služieb v oblasti ochrany osobných údajov a oblasti autorského práva a práva IT.

- IT-TECH SERVICES s.r.o. –systémový integrátor a zaoberá sa návrhom IT infraštruktúry a podporou koncových zákazníkov. Poskytuje podnikové riešenia pre komerčné subjekty a samosprávy.
- LDcentrum Computers s.r.o. – spoločnosť zaoberajúca sa správou a návrhom IT infraštruktúry, podporou koncových zákazníkov, IoT a podnikovými riešeniami, a tiež pôsobiaca ako systémový integrátor.
- LD - Power, s. r. o. – výrobca a dodávateľ elektrickej energie z obnoviteľných zdrojov.
- Mesto Holíč.
- Obec Limbach.
- Salutis Systems, a. s. – spoločnosť zaoberajúca sa výskumom a vývojom v oblasti šifrovania dát.
- Správa IT s. r. o. – spoločnosť zaoberajúca sa správou IT, integrátor riešení IKT pre klientov verejnej správy (ITVS).
- Stredná odborná škola elektrotechnická Liptovský Hrádok.
- TAYLLOR & COX Slovensko, a.s. - spoločnosť poskytujúca komplexné služby v oblasti systémových ISO certifikácií, auditov, školení a expertných posudkov, prevádzkujúca vlastný elektronický aukčný systém.
- TÜV SÜD Slovakia s.r.o. - poskytuje služby v oblastiach certifikácie, inšpekcie a vzdelávania, pôsobí vo všetkých odvetviach priemyslu a služieb.

2.2.3 *Predmet činnosti*

Cluster Kybernetickej Bezpečnosti, vďaka rozmanitosti svojich členov a ich dlhoročných skúseností na trhu, vytvára podmienky pre rozvoj kybernetickej bezpečnosti v Slovenskej republike.

Svojou činnosťou zvyšuje informovanosť podnikateľského prostredia, verejnej správy a samospráv o dôležitosti kybernetickej bezpečnosti, apeluje na potrebu venovať sa téme ochrany dát. Poskytuje pomoc v procese zavádzania a následnej realizácie nevyhnutných bezpečnostných opatrení v súvislosti s plnením zákonných požiadaviek v oblasti kybernetickej bezpečnosti. Monitoruje a analyzuje jednotlivé sektory hospodárstva pri plnení požiadaviek zákona o kybernetickej bezpečnosti a upozorňuje na prípadné nedostatky.

Od svojho vzniku, Cluster Kybernetickej Bezpečnosti organizoval viaceré konferencie, workshopy a semináre a tým prispel k zvýšeniu informovanosti všetkých zainteresovaných strán o kybernetickej bezpečnosti. Organizovaním vzdelávacích programov a iných foriem osvetovej činnosti v oblasti kybernetickej bezpečnosti, klaster približuje a zdieľa s verejnosťou najnovšie informácie z oblasti IT. Vytvára komplexné riešenia pre subjekty, ktoré chcú alebo majú zákonnú povinnosť implementovať bezpečnostné opatrenia pre oblasť ochrany dát.

Vstupom do „Únie klastrov Slovenska“ sa Cluster Kybernetickej Bezpečnosti aktívne zapojil do komunikácie klastrových organizácií z iných odvetví a podporil tým medziodvetvovú spoluprácu v regiónoch Slovenska

2.2.4 *Štruktúra, riadenie a financovanie činnosti*

Orgánmi Clustra Kybernetickej Bezpečnosti sú valné zhromaždenie a predseda, ktorým bol na prvé obdobie zvolený Ing. Ján Lichvár. Valné zhromaždenia ako najvyšší orgán schvaľuje zásadné rozhodnutia a mimo iné

rozhoduje vo veciach prijímania nových členov. Funkcia predsedu je predovšetkým v rovine riadiacej a organizačnej.

Praktická spolupráca členov klastra prebieha zvyčajne vytvorením mikroteamov pre plnenie špecifických potrieb klientov, s využitím ad – hoc potrebných špecializácií členov.

Okrem pravidelných stretnutí na valnom zhromaždení, jednotliví členovia podľa potrieb iniciujú ďalšie osobné i telekonferenčné stretnutia v širšom, alebo užšom kruhu. Pravidelná osobná komunikácia členov umožňuje rýchlu reakcia na aktuálne požiadavky klientov.

Financovanie aktivít Clustra Kybernetickej Bezpečnosti je zabezpečené zo vstupných poplatkov a ročného členského poplatku, ktorého výška je každoročne odsúhlasená na valnom zhromaždení.

2.2.5 *Predmet činnosti*

Cluster Kybernetickej Bezpečnosti, vďaka rozmanitosti svojich členov a ich dlhoročných skúseností na trhu, vytvára podmienky pre rozvoj kybernetickej bezpečnosti v Slovenskej republike.

Svojou činnosťou zvyšuje informovanosť podnikateľského prostredia, verejnej správy a samospráv o dôležitosti kybernetickej bezpečnosti, apeluje na potrebu venovať sa téme ochrany dát. Poskytuje pomoc v procese zavádzania a následnej

realizácie nevyhnutných bezpečnostných opatrení v súvislosti s plnením zákonných požiadaviek v oblasti kybernetickej bezpečnosti. Monitoruje a analyzuje jednotlivé sektory hospodárstva pri plnení požiadaviek zákona o kybernetickej bezpečnosti a upozorňujeme na prípadné nedostatky.

Od svojho vzniku, Cluster Kybernetickej Bezpečnosti organizoval viaceré konferencie, workshopy a semináre a tým prispel k zvýšeniu informovanosti všetkých zainteresovaných strán o kybernetickej bezpečnosti. Organizovaním vzdelávacích programov a iných foriem osvetovej činnosti v oblasti kybernetickej bezpečnosti, klaster približuje a zdieľa s verejnosťou najnovšie informácie z oblasti , i. Vytvára komplexné riešenia pre subjekty, ktoré chcú alebo majú zákonnú povinnosť implementovať bezpečnostné opatrenia pre oblasť ochrany dát. Vstupom do „Únie klastrov Slovenska“ sa Cluster Kybernetickej Bezpečnosti aktívne zapojil do komunikácie klastrových organizácií z iných odvetví a podporil tým medziodvetvovú spoluprácu v regiónoch Slovenska.

2.2.6 *Marketing*

Keďže financovanie aktivít klastra je zabezpečené takmer výlučne formou vstupných poplatkov a členských poplatkov, možnosti viesť plnohodnotnú a aktívnu informačnú kampaň a dosiahnuť vytýčené ciele je obmedzená.

Vzhľadom na obmedzené prostriedky, používajú členovia k propagácii osobný networking a profesijnú sociálnu sieť. Na propagačné aktivity členov následne nadväzuje už vyššie zmienené organizovanie tematických konferencií a workshopov.

2.3 SWOT analýza Clustra Kybernetickej Bezpečnosti

STRENGHTS / Silné stránky	WEAKNESSES / Slabé stránky
• Vysoká miera odbornosti v súvislosti s variabilitou členov. • Komplexné vypracovanie dokumentácie na základe individuálnych potrieb cieľového subjektu, právne analýzy v súvislosti s GDPR. • Zvyšovanie povedomia a informovanosti o potrebe zachovania stavu kybernetickej bezpečnosti, monitorovanie a analyzovanie stavu kybernetickej bezpečnosti, návrhy nápravných opatrení. • Návrhy inovácií na základe najnovších poznatkov v oblasti kybernetickej bezpečnosti. • Vypracovanie metodiky pre postup forenznej analýzy v prípade kybernetického útoku. • Poskytovanie komplexného riešenia bezpečnosti pre oblasť digitalizácie spoločností. • Vysoká miera flexibility pre ochranou pred hrozbami možných útokov na infraštruktúru subjektov (verejný a súkromný sektor). • Organizácia workshopov, konferencií pre prevádzkovateľov základnej služby k otázkam plnenia povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti. • Podpora osvety a vzdelávania v súvislosti s kybernetickými hrozbami na úrovni stredného školstva. • Spolupráca s vysokými školami na inováciách pre implementácie v oblasti kybernetickej bezpečnosti.	• Financovanie z externých zdrojov. • Nedostatok odborných ľudských zdrojov. • Nízke povedomie verejnej aj súkromnej sféry v súvislosti s klastrovými organizáciami. • Nízke povedomie verejnej aj súkromnej sféry o potrebe ochrany pred kybernetickými hrozbami.
OPPORTUNITIES / Príležitosti	**THREATS / Hrozby**
• Spoločné vzdelávacie aktivity medzi členmi klastra. • Zviditeľnenie spolupráce a prezentácia jednotlivých členov CKB v rámci klastrových organizácií. • Projekty so strednými školami a vysokými školami s technickým zameraním. • Prezentácia a realizácia duálneho vzdelávania. • Prezentácia na medzinárodnom fóre. • Financovanie z vonkajších zdrojov, na podporu osvetovej činnosti a vzdelávania.	• Podceňovanie hrozieb kybernetických útokov. • Ekonomické dopady pandémie spôsobené ochorením COVID – 19. • Podceňovanie hrozieb kybernetických útokov. • Nesúlad deklarovaných a skutočných profesijných vedomostí u konkurencie. • Deklaratórne vymáhanie sankcií v oblasti zákonných povinností. • Absencia duálneho vzdelávania v oblasti kybernetickej bezpečnosti.

3 Poslanie, vízia, stanovenie cieľov a priorít

3.1 Poslanie a vízia

Poslaním Clustra Kybernetickej Bezpečnosti je zlepšovať informovanosť verejnej správy, samospráv a podnikateľského prostredia o dôležitosti problematiky kybernetickej bezpečnosti vo vzťahu k prevádzke infraštruktúry (software, hardware, aplikácie a siete) týchto subjektov. Potrebné je zvyšovať povedomie v oblasti kybernetickej bezpečnosti pre všetky sektory, úrovne, oblasti a rôznorodosti prostredia a zamerať sa na zabezpečenie ochrany dátových aktív. V súvislosti so zákonom o kybernetickej bezpečnosti, na úrovni celej organizácie a jednotlivých členov, sa orientujeme na pomoc prevádzkovateľom základnej služby, ako aj iným subjektom v uľahčení návrhu a následnej realizácie potrebných bezpečnostných opatrení.

Využitím potenciálu vzájomnej spolupráce medzi klastrami a inými subjektami na regionálnej a národnej úrovni hľadáme spôsob ako sa efektívne prepájať a komunikovať medzi rôznymi sektormi. Vďaka členstvu v Únii klastrov Slovenska sa nielen pre Cluster Kybernetickej Bezpečnosti, ale aj pre iných členov otvára možnosť ako zmeniť vnímanie klastrov, nielen na regionálnej úrovni, ale na celom území Slovenska.

Na základe odporúčania v hodnotiacej správe z procesu certifikácie spoločnosťou European Secretariat for Cluster Analysis (ESCA) plánuje klaster svoje aktivity, spoluprácu a výmenu informácií rozšíriť nielen o nových partnerov zo Slovenskej republiky, ale i z našich najbližších susedských štátov (krajiny V4).

Svojou činnosťou iniciuje aktívnu spoluprácu s dôrazom na potrebu sieťovania podnikov a celkovú medziodvetvovú spoluprácu. Týmto spôsobom pomáha riešiť spoločenské výzvy, snaží sa vytvárať transparentnejšie prostredie a v súvislosti so združovaním malých a stredných organizácií, umožňuje aj menším hráčom na trhu s bohatými skúsenosťami, presadiť sa.

Vzhľadom na prebiehajúcu spoluprácu medzi podnikateľskou sférou, vedecko-výskumnou základňou, štátnymi orgánmi, samosprávami a neziskovým sektorom, klaster podporuje prostredníctvom inovácií, nielen rozvoj jedného územia (regiónu), ale aj ostatných regiónov v Slovenskej republike.

Vyššie uvedené ciele má podporiť vytvorenie centra excelentnosti, ktoré bude slúžiť všetkým členom klastra na praktické ukážky moderných technológií: moderného hardware vybavenia a inovatívneho a pokrokového softwarového vybavenia na monitoring kybernetickej bezpečnosti. Členovia klastra sa do tvorby centra zapoja najmä poskytnutím svojho know how. Každý člen klastra sa bude môcť dôkladnejšie oboznámiť s predmetom činnosti iných členov a členovia získajú prehľad o celom spektre technických, procesných a právnych činností v oblasti kybernetickej bezpečnosti, ktoré jednotliví členovia vykonávajú.

Prípravou konferencií a webinárov pre iné klastrové organizácie a prevádzkovateľov základnej služby zvýšime informovanosť, všeobecný rozhľad so zameraním na aktualizácie a zmeny legislatívy v oblasti ochrany dátových aktív.

Pre plnenie povinností prevádzkovateľov základnej služby podľa zákona číslo 69/2018 Z. z. pre , vidia členovia klastra zmysel pokračovať v realizácii workshopov.

Je žiadúce ich pripraviť individuálne na základe sektorových potrieb a s prihliadnutím na odlišnosti plnenia opatrení v jednotlivých sektoroch, či už na úrovni technickej, alebo právnej. Nie je možné vypracovať súhrnnú odvetvovú metodiku pre každú oblasť. Z uvedeného dôvodu je nevyhnutné v spolupráci s členmi Clustra Kybernetickej Bezpečnosti na workshopoch informovať subjekty spadajúce pod jednotlivé sektory a členov ďalších klastrových organizácií v iných regiónoch, o špecifikách pre dané sektory. Cieľom klastra je príprava každoročných workshopov podľa sektorov: Bankovníctvo; Doprava; Elektronické komunikácie; Energetika; Infraštruktúra finančných trhov; Pošta; Priemysel; Voda a atmosféra; Verejná správa; Zdravotníctvo. Priebeh realizácie jednotlivých workshopov úzko súvisí so spoluprácou na sektorovej úrovni, so zapojením príslušných asociácií a profesijných združení. Preferovaná bude prezenčná forma, nakoľko osobná interakcia je prospešná a často len ťažko nahraditeľná. Nevyhnutnou súčasťou je kvalitná marketingová činnosť, spojená s prípravou, oslovením cieľových účastníkov, a následnou publikáciou výsledkov jednotlivých workshopov.

Vychádzajúc z hodnotiacej správy pri procese certifikácie spoločnosťou European Secretariat for Cluster Analysis (ESCA) vedenie a samotní členovia vnímajú potrebu neustále podporovať spoločné činnosti členov klastra, nad rámec aktívnej komunikácie členov , či už pri spolupráci v mikroteamoch, prípadne na spoločných stretnutiach a valných zhromaždeniach. Pripravujeme spoločne návštevy centier riadenia monitoringu kybernetickej bezpečnosti, odborné vzdelávacie aktivity podnecujú jednotlivých členov klastra ku kontinuálnemu vzdelávaniu a zdokonaľovaniu sa.

V procese digitalizácie je zásadné venovať sa zvyšovaniu odbornosti a prevedeniu nových poznatkov do praxe. Zvyšovaniu odbornosti pomáha konfrontácia

so zahraničím, účasťou na konferenciách s celosvetovými špičkami v oblasti ochrany dátových aktív a prezentovania ich skúseností vidíme jedinečnú možnosť ako osobne nadviazať spoluprácu, vymeniť si poznatky, preniesť informácie a tieto skúsenosti do svojej činnosti a tým zvýšiť kvalitu ochrany dátových aktív v Slovenskej republike.

Víziou Clustra Kybernetickej Bezpečnosti je pomocou aktívnej spolupráce členov pri vzdelávacích aktivitách, zvýšiť ich profesijnú odbornosť v oblasti ochrany dátových aktív a kybernetickej bezpečnosti, aby ju členovia zdieľali so zástupcami ďalších sektorov a podnietili ich k aktivite, výmene skúseností a záujmu o vzdelávanie sa. Prehĺbením komunikácie so zástupcami klastrových organizácií v iných regiónoch a odvetviach vidíme veľký potenciál. Na základe spoločne stanovených tém sa klaster chce stať súčasťou pracovných skupín na Ministerstve investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a odovzdať tak skúsenosti z reálneho poskytovania služieb v oblasti kybernetickej bezpečnosti a ochrany dátových aktív štátnej správe. Týmto procesom plánujeme vyvolať odbornú diskusiu a tým skvalitniť prípravu strategických plánov, a legislatívy v Slovenskej republike.

3.2 Ciele

Cieľom Clustra Kybernetickej Bezpečnosti je uskutočnenie aktivít, ktoré prispejú k rozvoju vzájomnej komunikácie členov, zvýšia ich odbornosť a podnietia rozširovanie členskej základne klastra.

3.2.1 *Vytvorenie Centra excelentnosti kybernetickej bezpečnosti*

Vytvorenie centra excelentnosti bude slúžiť všetkým členom klastra na praktické ukážky moderných technológií v rozsahu moderného hardware vybavenia a inovatívneho a pokrokového softwarového vybavenia určeného pre monitoring kybernetickej bezpečnosti.

Členovia klastra sa do tvorby centra zapoja najmä poskytnutím svojho know how. Každý člen klastra sa bude môcť dôkladnejšie oboznámiť s predmetom činnosti iných členov a členovia získajú prehľad o celom spektre technických, procesných a právnych činností v oblasti kybernetickej bezpečnosti, ktoré jednotliví členovia vykonávajú.

Vytvorenie centra spája členov organizácie k pravidelným stretnutiam a napomáha dosiahnutiu vzájomnej synergie. Postupnými krokmi sa tvorí ucelené riešenie vznikajúceho centra. Získaním komplexného obrazu o činnostiach spojených s ochranou dátových aktív, členovia klastra získavajú predpoklady pre šírenie osvety (v oblasti kybernetickej bezpečnosti) aj na regionálnej úrovni, pri nadväzovaní kontaktov s inými klastrovými organizáciami. Vybudovaním centra excelentnosti podnietime členov klastra k neustálemu vzdelávaniu sa a inováciám.

Prezentáciou centra sa klastrová organizácia bude usilovať preniknúť do povedomia študentskej obce na úrovni stredoškolského a vysokoškolského vzdelávania, a podporovať študentov s cieľom zvýšiť ich záujem o prudko sa rozvíjajúcu oblasť kybernetickej bezpečnosti. Aktuálny nedostatok odbornej pracovnej sily na pracovnom trhu je trendom, ktorý spoločnosť smeruje k nevyhnutnému návratu k profilovaniu vo vzdelávaní aj vo formách duálneho a kontinuálneho vzdelávania. Noví členovia klastra z akademického prostredia sú zárukou rozvoja aktívnej participácie na vzdelávacom procese inovatívneho vzdelávania. Cieľ a želaný výsledok je zvyšovanie zamestnanosti v oblasti kybernetickej bezpečnosti.

3.2.2 *Vzdelávanie členov, nadviazanie spolupráce s novými partnermi, internacionalizácia*

Jedným z predpokladov rozvoja úrovne expertízy členov klastra je účasť na významných zahraničných konferenciách a veľtrhoch, prednostne s témou kybernetickej bezpečnosti. Výmena informácií, skúseností z implementácie a inovácií v oblasti kybernetickej bezpečnosti v zahraničí prispieva k presadzovaniu inovácií v tejto oblasti aj v Slovenskej republike.

Cieľom Clustra Kybernetickej Bezpečnosti je prezentovať, vzdelávať a šíriť osvetu o potrebe zvyšovania úrovne kybernetickej bezpečnosti na regionálnej a národnej úrovni a osloviť čo najširšiu masu užívateľov digitálnych technológií.

Nástrojom pre dosiahnutie cieľov klastra je tiež prepojenie klastrov podobného zamerania na nadnárodnej úrovni a to v prvom kroku vo Vyšehradskom regióne (Česká republika, Maďarsko, Poľsko, Slovenská republika). Medzinárodné prepojenie klastrov a medzinárodná výmena skúseností, nielen z oblasti

kybernetickej bezpečnosti, spolupráca v rámci už zabehnutej klastrovej politiky v zahraničí, umožní priniesť ďalšie inovatívne metódy práce v oblasti do národného prostredia.

Všetky vyššie spomenuté činnosti reflektujú odporúčania z procesu certifikácie našej organizácie spoločnosťou European Secretariat for Cluster Analysis (ESCA).

3.2.3 *Vzdelávacie, odborné, informačné a osvetové podujatia*

Organizovaním vzdelávacích, odborných a informačných ako aj osvetových podujatí sa zameriavame na výmenu informácií medzi klastrovými organizáciami z celého Slovenska. Jednotliví členovia a iní účastníci majú v tejto komunite možnosť čerpať a vymieňať si informácie k novým postupom, byť informovaní o zmenách v relevantnej legislatíve. Vidíme veľký potenciál v komunikácii klastrových organizácií medzi regiónmi v súvislosti ich rozdielnosti (hospodárstvo, ľudské zdroje, finančné zdroje). Na základe spoločne stanovených tém sa chceme stať súčasťou pracovných skupín na Ministerstve investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a odovzdať naše skúsenosti z reálneho poskytovania služieb v oblasti kybernetickej bezpečnosti a ochrany dátových aktív štátnej správe. Chceme vyvolať odbornú diskusiu a skvalitniť prípravu strategických plánov a legislatívy v Slovenskej republike.

V súvislosti s plnením podmienok zákona číslo 69/2018 Z. z. pre prevádzkovateľov základnej služby budeme pripravovať workshopy pre jednotlivé sektory, menovite: Bankovníctvo; Doprava; Elektronické komunikácie; Energetika; Infraštruktúra finančných trhov; Pošta; Priemysel; Voda a atmosféra; Verejná správa; Zdravotníctvo. Každé z menovaných odvetví má svoje špecifiká a v súvislosti

s plnením požiadaviek je potrebné sústrediť sa práve na tieto špecifiká , či už na úrovni technickej, alebo legislatívnej. Nie je možné vypracovať súhrnnú odvetvovú metodiku a z uvedeného dôvodu považujeme za nevyhnutné v spolupráci s členmi klastra informovať subjekty spadajúce pod jednotlivé sektory a taktiež členov klastrových organizácií v iných regiónoch. Tento spôsob máme odskúšaný aj z minulosti a na základe pozitívnych reakcií sa chceme zamerať na nové workshopy s publikom na regionálnej úrovni aj v iných častiach Slovenska, ktoré spája rovnaká sektorová príslušnosť. Priebeh realizácie jednotlivých workshopov úzko súvisí so spoluprácou na sektorovej úrovni za angažovania príslušných asociácií a profesijných združení. Našou prioritou je každý workshop realizovať na prezenčnej báze. Nevyhnutnou súčasťou prípravy workshopov je marketingová činnosť, spojená s prípravou, oslovením cieľových účastníkov, realizáciou a následnou publikáciou výsledkov jednotlivých workshopov.

3.3 Súlad cieľov Clustra Kybernetickej Bezpečnosti so stratégiou výskumu a inovácií pre inteligentnú špecializáciu Slovenskej republiky (RIS 3 SK)

Slovenská republika v úmysle podporiť konkurenčnú schopnosť, zamestnanosť a kvalitu života zamerala svoju pozornosť na podnietenie celkovej zmeny ekonomiky, založenej na inovačnom rozvoji a výskumnej excelentnosti. Na týchto základoch bola postavená aj tvorba Stratégie výskumu a inovácií pre inteligentnú špecializáciu SR (RIS3 SK). Jadrom stratégie je cielená podpora a stimulácia verejno-súkromnej výskumno-vývojovej a inovačnej spolupráce, uvoľňujúcej možnosti rastu pre všetkých zainteresovaných účastníkov.

RIS3 SK, schválená uznesením vlády SR č. 665/2013 dňa 13. 11. 2013, stanovuje investičné a štrukturálne opatrenia pre politiku výskumu, vývoja a inovácií. Riadiacim orgánom implementácie RIS3 SK je Rada vlády Slovenskej republiky pre vedu, techniku a inovácie, ktorej prierezovým, pracovným, koordinačným a komunikačným orgánom je Stála komisia Rady vlády SR pre vedu, techniku a inovácie pre implementáciu RIS3.

OP Výskum a inovácie predstavuje hlavný implementačný nástroj RIS3 SK a prvý spoločný programový dokument Ministerstva školstva, vedy, výskumu a športu SR a Ministerstva hospodárstva SR, spájajúci a definujúci podporu výskumu, vývoja a inovácie z európskych štrukturálnych a investičných fondov (EŠIF). Niektoré programy EŠIF a programy financované zo štátneho rozpočtu sa na napĺňaní cieľov RIS3 SK podieľajú v menšom meradle (*1) .

Činnosťou a inováciami, Cluster Kybernetickej Bezpečnosti, chce a vie prispieť ku koordinácii činností, navrhnúť a podporiť realizáciu činností podľa požadovanej produktovej línie, „Kybernetická bezpečnosť a bezpečný prenos údajov v priemyselnom prostredí“ vychádzajúcej z RIS 3, viď. dokument Produktové línie pre doménu Digitálne Slovensko a kreatívny priemysel, str. 26 : Hlavný trend „I. Priemysel 4.0, Vedľajší trend „2. Bezpečnosť a komunikácia (v priemysle)“, Produktová línia “ Kybernetická bezpečnosť a bezpečný prenos údajov v priemyselnom prostredí (*2).

4 Akčné plány

4.1 Akčný plán 1 - vytvorenie Centra excelentnosti kybernetickej bezpečnosti

4.1.1 *Priebeh*

Priebeh od prípravného procesu k realizácii pozostáva z krokov, ktoré na seba nadväzujú:

- komplexné plánovanie centra,
- vytvorenie primeraného priestoru pre centrum,
- obstaranie hardware vybavenia,
- obstaranie software vybavenia,
- implementácia, know how jednotlivých členov v oblasti právnej, procesnej a technickej,
- začatie prevádzky centra,
- využívanie centra členmi klastra na získanie komplexného obrazu o činnostiach spojených s ochranou dát,
- šírenie osvety členmi klastra na základe získaných nových poznatkov aj na regionálnej úrovni,
- nadviazanie nových kontaktov v iných klastrových organizáciách a s inými subjektmi,
- vyvolanie spolupráce s akademickou obcou s následným dôrazom na duálne a kontinuálne vzdelávanie,
- inovovanie centra na základe nových trendov a metód,
- spracovanie požiadaviek členov na vylepšenie činnosti,

- hodnotenie prevádzky centra a príprava podkladov pre prednesenie ročnej správy na valnom zhromaždení.

4.1.2 *Časový harmonogram*

- Prípravný proces: 07/2021 – 12/2021.
- Vytvorenie a otvorenie prevádzky: 01/2022 – 04/2022.
- Realizácia vzdelávania na všetkých úrovniach: 05/2022 – 12/2023.
- Inovácia centra: 05/2022 – kontinuálne bez časového limitu.

4.1.3 *Financovanie*

- Viazané na príspevky členov Clustra Kybernetickej Bezpečnosti a z cudzích zdrojov.

4.1.4 *Personálne zabezpečenie*

Sústredenie sa na podporu zamestnania v regióne a vytvorenie viacerých pozícií s rozdielnym fondom pracovného času (aj úväzky na skrátený pracovný úväzok) pri porovnateľnej efektívnosti ich činnosti. Výber bude zameraný na pracovníkov odborne zdatných s praxou a preukázateľnosťou kvalifikácie, ktorí budú nevyhnutnou súčasťou odborného teamu. Pre kvalitné fungovanie a podporu rastu medziklastrovej spolupráce je žiadúci výber aktívnych a efektívne pracujúcich zamestnancov, kde im klaster vie ponúknuť možnosť vzdelávať sa, kariérne rásť a zapojiť sa do moderných trendov v oblasti digitalizácie. S vyšším počtom zamestnancov vie klastrová organizácia aktívne reagovať na zmeny a je

schopná presunúť pracovnú silu na plánované činnosti, tak aby to bolo efektívne i hospodárne a v neposlednom rade bez ťažkostí možné zvládnuť proces zastupiteľnosti.

- Výber zodpovedných pracovníkov bude prebiehať v roku 2021 na úrovniach projektových riadiacich pracovníkov, realizačných pracovníkov a administratívnych pracovníkov.

4.2 Akčný plán 2 - vzdelávanie členov a nadviazanie spolupráce, internacionalizácia

4.2.1 *Priebeh*

- komplexné plánovanie jednotlivých vzdelávacích činností súvisiacich s každoročnou účasťou na významných medzinárodných konferenciách s tematikou kybernetická bezpečnosť a prehliadky dátových centier: zabezpečenie vstupeniek na konferencie, zabezpečenie prehliadok dátových centier, zabezpečenie ubytovania, zabezpečenie dopravy, oslovenie účastníkov, príprava podkladov pre účastníkov,
- realizácia,
- príprava hodnotiaceho procesu zo vzdelávacej činnosti,
- zostavenie správy,
- príprava podkladov na implementáciu inovatívnych metód do Centra excelentnosti kybernetickej bezpečnosti,
- začatie komunikácie so získanými kontaktami z rady iných klastrových organizácií a iných subjektov,
- nadviazanie medzinárodnej spolupráce z rady iných klastrových organizácií a iných subjektov,
- spracovanie požiadaviek členov na vylepšenie činnosti a vzdelávacích aktivít,
- príprava podkladov pre prednesenie ročnej správy na valnom zhromaždení.

Zoznam plánovaných účastí na medzinárodných konferenciách:

- *Česká Republika, Praha: QuBIT 2021,*
- *Česká Republika, Praha: QuBIT 2022,*
- *Česká Republika, Praha: QuBIT 2023.*

Účasťou členov klastra na tejto prestížnej konferencii v Českej republike je, pravidelne, každý rok zúčastniť najbližšie dostupnej kvalitnej konferencie s témou kybernetická bezpečnosť. Stretnutím so špičkami českých a slovenských predstaviteľov chceme získať nové vedomosti a taktiež nových partnerov na spoluprácu z Českej republiky. Našou snahou, je internacionalizácia a výmena informácií s predstaviteľmi organizácií klastrového typu v krajinách V4. Z hľadiska dostupnosti a kvality je táto konferencia plánovaná ako nevyhnutná súčasť našej činnosti. Pridaná hodnota pre našich klastrových partnerov v Slovenskej republike je neodškriepiteľná, nakoľko konferencie podobného charakteru, veľkosti, kvality žiaľ v Slovenskej republike nemáme. Členovia klastra budú môcť každý vidieť a zažiť inovácie o ktorých by sa na slovenskom fóre inak len diskutovalo.

- *Česká Republika: Konference Security 2021,*
- *Česká Republika: Konference Security 2022,*
- *Česká Republika: Konference Security 2023.*

Konference Security má v Českej republike svoje stále miesto. Okrem toho, že sa chceme zúčastniť konferencie a čerpať nové informácie z Českej republiky v oblasti informačnej bezpečnosti, máme aj ambície aktívne sa zúčastniť a prezentovať naše poznatky a skúsenosti zo Slovenskej republiky. Práve na odbornom fóre tohto rozsahu nájdeme nových partnerov pre spoluprácu z Českej republiky a budeme schopní zvýšiť frekvenciu výmeny informácií aj s novými partnermi.

- *Česká Republika: Konference IDC Security Forum 2021,*
- *Česká Republika: Konference IDC Security Forum 2022,*

- *Česká Republika: Konference IDC Security Forum 2023.*

Konference IDC Security Forum v roku 2021 bude tak slúžiť pre čerpanie nových informácií ako aj pre prezentáciu našich členov z oblasti kybernetickej bezpečnosti. Jedná sa o aktívne stretnutia s partnermi s ktorými spolupracujeme v súčasnosti a na tomto fóre si vymieňame praktické skúsenosti zo svojej činnosti.

- *Veľká Británia, Londýn: Info Security London 2021,*
- *Veľká Británia, Londýn: Info Security London 2022,*
- *Veľká Británia, Londýn: Info Security London 2023.*

Stretnutie s celosvetovými špičkami v oblasti ochrany bezpečnostných aktív prinesie nové poznatky a skúseností zo sveta kybernetickej bezpečnosti. Je to prestížna celosvetová konferencia, ktorá každý rok prinesie do Londýna to najkvalitnejšie. Info Security London je jedinečná a dostupná možnosť pre našich účastníkov osobne nadviazať spoluprácu, vymeniť si poznatky, preniesť informácie a tieto skúsenosti do svojej činnosti a tým zvýšiť kvalitu v procesoch ochrany dátových aktív v Slovenskej republike.

Zoznam plánovaných návštev dátových centier:

- *Návšteva Security Operation Center – „SOC“ O2 Security Expert Center v Prahe.*

Návšteva tohto vysoko špecializovaného pracoviska v Českej republike umožní v krátkom čase predstaviť, ako sa takéto špecializované pracovisko

dokáže postarať o ochranu dátových aktív a permanentne dohliadať a spravovať dátové aktíva. Súvislosť návštevy O2 Security Expert Center v Prahe je práve vo vybudovaní Centra excelentosti v Slovenskej republike.

- *Návšteva Kybernetického polygónu KYPO na Masarykovej univerzite v Brne.*

Kybernetický polygón na Masarykovej univerzite chceme navštíviť a využiť jeho potenciál ako jedinečný príklad spolupráce akademickej obce. Toto výučbové centrum aj účastníkom klastra, ktorí doposiaľ nemali skúsenosť s kybernetickým incidentom, predstaví ako môže incident nastať a akým spôsobom je vhodné postupovať.

- *Návšteva centra CISCO v Krakove v Poľskej republike.*

Spoločnosť CISCO je známa ako svetový líder v oblasti kybernetickej bezpečnosti sietí a aktívnych prvkov. Nakoľko práca s ochranou dátových aktív je založená aj na produktoch CISCO, ktoré sú v Slovenskej republike vo verejnom sektore výrazne zastúpené, je potrebné sa pravidelne zúčastňovať na komunikácii so zástupcami tejto spoločnosti a oboznámiť sa s inováciami v portfóliu spoločnosti. Vzhľadom na kvalitu produktov (hardware, software, ...) sú často integrované do procesov ochrany dátových aktív pre subjekty v Slovenskej republike. Osobným kontaktom s partnermi z Poľskej republiky si chceme zabezpečiť pravidelnú komunikáciu, spoluprácu a taktiež ich účasť na plánovaných workshopoch a webinároch v Slovenskej republike.

4.2.2 *Časový harmonogram*

- 07/2021 – 12/2023

4.2.3 *Financovanie*

- Viazané na príspevky členov Clustra Kybernetickej Bezpečnosti a z cudzích zdrojov.

4.2.4 *Personálne zabezpečenie*

- Výber zodpovedných pracovníkov bude prebiehať v roku 2021 na úrovniach projektových pracovníkov a administratívnych pracovníkov.

4.3 *Akčný plán 3 - vzdelávacie, odborné, informačné a osvetové podujatia*

- *Sektorové workshopy pre prevádzkovateľov základnej služby podľa zákona č. 69/2018 Z. z., pre jednotlivé sektory, menovite: Bankovníctvo; Doprava; Elektronické komunikácie; Energetika; Infraštruktúra finančných trhov; Pošta; Priemysel; Voda a atmosféra; Verejná správa; Zdravotníctvo.*

- *Konferencie a webináre pre iné klastrové organizácie a ďalších prevádzkovateľov základnej služby.*

4.3.1 *Priebeh*

- komplexné plánovanie jednotlivých podujatí so zreteľom na sektorovú odlišnosť (každoročne),
- oslovenie zástupcov jednotlivých sektorov a príslušných asociácií,
- koncepcia programu,
- príprava podkladov k vzdelávaniu (materiály, prezentácia, marketingové podklady),
- výber priestorov realizácie podujatí,
- zabezpečenie podujatí po personálnej, odbornej a technickej stránke,
- realizácia,
- príprava hodnotiaceho procesu zo vzdelávacieho podujatia,
- príprava a publikovanie výsledkov,
- zostavenie správy,
- začatie komunikácie so získanými kontaktami z rady iných klastrových organizácií a iných subjektov,

- nadviazanie spolupráce s členmi iných klastrových organizácií a inými subjektmi,
- spracovanie požiadaviek aktérov podujatia na vylepšenie vzdelávacích aktivít,
- príprava podkladov pre prednesenie ročnej správy na valnom zhromaždení.

4.3.2 *Časový harmonogram*

- 07/2021 – 12/2023

4.3.3 *Financovanie*

- Viazané na príspevky členov Clustra Kybernetickej Bezpečnosti, z cudzích zdrojov.

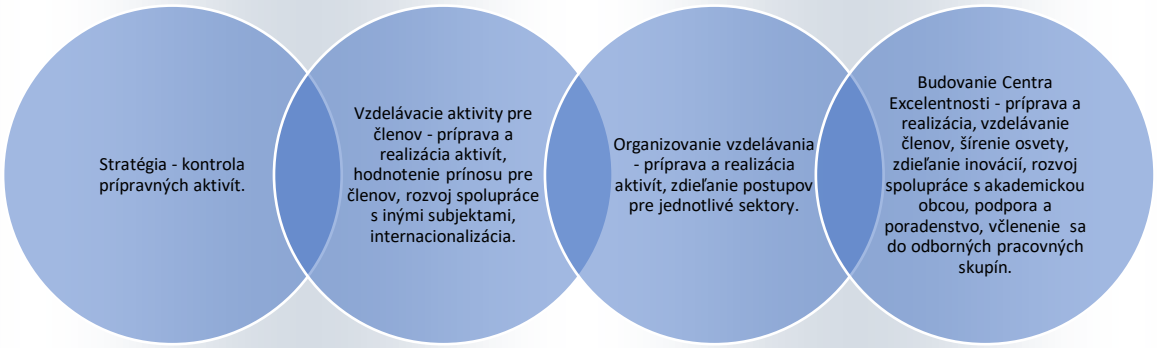
4.3.4 *Personálne zabezpečenie*

- Výber zodpovedných pracovníkov bude prebiehať v roku 2021 na úrovniach projektových pracovníkov, administratívnych pracovníkov.

5 Kontrolný mechanizmus

Súčasťou kontrolného mechanizmu pri procese vyhodnotenia jednotlivých činností bude priebežný proces kontroly medzi zainteresovanými členmi klastra.

Vytvorením štruktúry a jasným zadefinovaním vzťahov a súvislostí medzi jednotlivými aktérmi riadenia a realizácie aktivít sa budeme snažiť o dosiahnutie želaného efektu pri plnení úloh s dôrazom na efektívnu činnosť, hospodárnosť a prínos nielen pre členov klastra. Sledované budú procesy vedúce k dosahovaniu plnenia cieľov vychádzajúcich zo stratégie:



Súčasťou kontrolného mechanizmu vyhodnotenia plnenia cieľov a súvisiacich čiastkových aktivít, ktoré sú potrebné k plneniu cieľov, bude pravidelné mesačné reportovanie činnosti.

Súhrnná ročná správa za realizované aktivity bude prezentovaná na valnom zhromaždení.

Pri kontrole a vyhodnotení činnosti bude dôležitým ukazovateľom správneho napredovania Clustra Kybernetickej Bezpečnosti i vzrastajúci záujem nových subjektov o členstvo v klastri a vytvorenie si stabilného miesta v kruhoch odbornej verejnosti v Slovenskej republike.

6 Záver

Pozitíva digitalizácie, najmä zvyšovanie efektivity práce a úspora času sú motiváciou pre Cluster Kybernetickej Bezpečnosti organizovať vzdelávanie vlastných členov ako aj širšej verejnosti v oblasti kybernetickej bezpečnosti.

Cieľom aktivít klastra je prostredníctvom odovzdávania skúseností, odborným poradenstvom a príkladmi z praxe, napomáhať v celej šírke sektorov hospodárstva, premene Slovenska na úspešnú, modernú a digitálnu krajinu.

Použité zdroje a literatúra

(*1) zdroj, https://www.opvai.sk/ris3/

(*2) zdroj, dokument Produktové línie pre doménu Digitálne Slovensko a kreatívny priemysel, str. 26 : Hlavný trend „I. Priemysel 4.0, Vedľajší trend „2. Bezpečnosť a komunikácia (v priemysle)“, Produktová línia “ Kybernetická bezpečnosť a bezpečný prenos údajov v priemyselnom prostredí; https://www.opvai.sk/media/99313/digit_creativ_domena_final_22032018_pp.pdf).