Strategie elektronické bezpečnosti Kraje Vysočina

2022 - 2025

tel.: 564 602 104, fax: 564 602 432, e-mail: posta@kr-vysocina.cz, internet: www.kr-vysocina.cz
IČ: 70890749,

Obsah

Úvod

Strategie elektronické bezpečnosti Kraje Vysočina 2022 – 2025 (dále jen Strategie) je jedním z dokumentů Kraje Vysočina reagující na vzrůstající význam problematiky elektronické bezpečnosti. Dokument představuje cíle a oblasti, které by měly vést ke zlepšení elektronické bezpečnosti dětí a studentů, rodičů i seniorů, pedagogů, běžných uživatelů internetu, organizací apod. z Kraje Vysočina.

Tento dokument obsahuje strategické záměry Kraje Vysočina týkající se problematiky elektronické bezpečnosti. Navazuje na Strategii elektronické bezpečnosti Kraje Vysočina 2018 – 2021. Strategie je vytvořena jako základní koncept aktivit pracovní skupiny elektronické bezpečnosti (dále jen pracovní skupiny) pro roky 2022 – 2025,[1] která na Krajském úřadě Kraje Vysočina působí již od roku 2010. Také by tato strategie měla sloužit jako základní dokument pro tvorbu dalších koncepčních materiálů týkajících se problematiky elektronické bezpečnosti.

Strategie je v souladu se základními dokumenty týkajícími se prevence kriminality a kybernetické kriminality v České republice. Jedná se následující dokumenty - Strategie prevence kriminality v České republice 2022 - 2027, Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025, Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 – 2025. Strategie vychází také z Koncepce prevence kriminality Kraje Vysočina na léta 2017 až 2022, kde je jedním z cílů omezování kriminality páchané prostřednictvím informačních a komunikačních technologií. Strategie je také v souladu se Strategií kybernetické bezpečnosti příspěvkových organizací zřizovaných Krajem Vysočina.

Strategie je rozčleněna do 3 částí. První část popisuje úlohu a postavení Kraje Vysočina v oblasti elektronické bezpečnosti a aktivity pracovní skupiny v období 2018 – 2021. Druhá část se zabývá analýzou problematiky elektronické kriminality v Kraji Vysočina a dosavadními aktivitami Kraje Vysočina v této oblasti. Třetí část přináší cíle a jednotlivé priority a aktivity v oblasti elektronické bezpečnosti v Kraji Vysočina na období 2022 - 2025.

[1] Na začátku každého roku připraví pracovní skupina Akční plán, který bude následně předán do Rady Kraje Vysočina (dále jen Rady) ke schválení. Současně bude také Radě předán dokument „Vyhodnocení akčního plánu“ z předchozího roku, který bude obsahovat přehled aktivit, které byly v daném roce splněny.

I. Úloha a postavení Kraje Vysočina v problematice el. bezpečnosti

Oblast rozvoje informačních technologií je dlouhodobě jednou z rozvojových priorit Kraje Vysočina. Intenzivní využívání informačních technologií ovšem vedle řady výhod přináší i rizika. Cílem Kraje Vysočina je především předcházet těmto rizikům. Proto také byla rozhodnutím vedení Kraje Vysočina v roce 2010 vytvořena odborná pracovní skupina pro elektronickou bezpečnost. Vedle pracovníků krajského úřadu z odborů informatiky, školství, sociálních věcí a sekretariátu hejtmana v ní jsou zástupci Policie ČR, hospodářské komory, Policejní akademie ČR v Praze, Vysočina Education (příspěvkové organizace Kraje Vysočina) či společnosti AUTOCONT a.s. Dále také zástupci sdružení CESNET, CZ.NIC a NÚKIB. Tato pracovní skupina se od roku 2010 schází v pravidelných dvouměsíčních intervalech a její členové se účastní i jednotlivých akcí organizovaných krajem v oblasti elektronické bezpečnosti.

Nebezpečí číhajících na uživatele internetu a dalších elektronických systémů a rizika spojená s jejich užíváním jsou velmi různorodá. Část této problematiky je zařazena mezi priority mnoha organizací na národní a mezinárodní úrovni. Jde zejména o problematiku porušování autorských práv, šíření nelegálního obsahu, síťové bezpečnosti a ekonomické kriminality. Mezi oblasti, které je dle názoru pracovní skupiny efektivní řešit na regionální úrovni patří zejména ochrana dětí a mládeže, seniorů, ohrožení malých a středních firem, preventivní akce pro odbornou veřejnost, shromažďování a vyhodnocování statistických dat souvisejících s elektronickou kriminalitou. Dále pak bezesporu vzdělávání cílových skupin v oblasti kyberbezpečnosti.

Další nepopiratelnou rolí kraje je péče o majetek a poskytování veřejné služby včetně jejich bezpečnosti. V tomto ohledu je pak důležitá práce s příspěvkovými organizacemi v oblasti bezpečnosti IT. Kraj Vysočina poskytuje pro své příspěvkové organizace řadu IT služeb včetně těch bezpečnostních. Nově také vznikla (2021) Strategie kybernetické bezpečnosti příspěvkových organizací zřizovaných Krajem Vysočina (dále jen „Strategie KB“), která je aplikovatelná právě na prostředí příspěvkových organizací zřizovaných Krajem Vysočina.

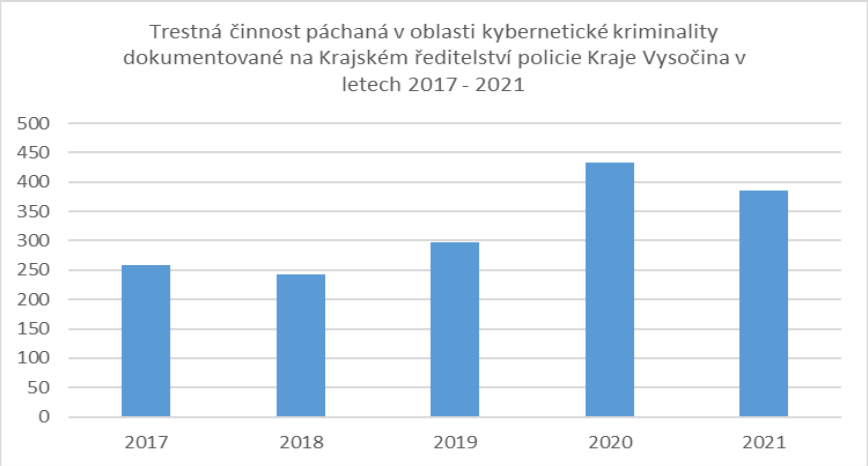
Krajský úřad Kraje Vysočina pak problematiku kybernetické bezpečnosti řeší organizačně i technicky ve vztahu ke klíčovým systémům kraje. V rámci úřadu je dlouhodobě zaveden systém řízení bezpečnosti (ISMS), úřad je certifikován dle normy ISO 27001/2015 a zřizuje několik pracovních pozic specializovaných na kybernetickou bezpečnost.

Kraj Vysočina se věnuje problematice elektronické bezpečnosti nejen na krajské úrovni, ale také na úrovni mezikrajské spolupráce v rámci projektu Kraje pro bezpečný internet. Projekt je realizován pod záštitou Asociace krajů České republiky. Jeho cílem je prostřednictvím spolupráce 13 krajů podporovat prevenci a vzdělávání v oblasti kyberbezpečnosti. Od roku 2016 je Kraj Vysočina vedoucím krajem projektu.

Kraj Vysočina je jedním z iniciátorů a signatářů memoranda o spolupráci v rámci tzv. hSOC iniciativy zaměřující se na bezpečnost v sektoru zdravotnictví. Hlavní myšlenkou této iniciativy je vytvoření bezpečné komunikační infrastruktury mezi nemocnicemi, lepší zabezpečení připojení k veřejném internetu, nastavení bezpečnostního monitoringu provozu, sdílení know-how a poskytování sdílených (distribuovaných) služeb včetně systémů pro včasné varování. Cílem je též i vytvoření jednotného incident response týmu, do kterého jsou aktivně zapojeni jak zástupci poskytovatelů zdravotních služeb, tak i bezpečnostních týmů, zástupci z oblasti vědy a výzkumu, vzdělávání, i poskytovatelé infrastruktury.

II. Analýza stavu elektronické bezpečnosti v Kraji Vysočina

Situace v oblasti elektronické bezpečnosti v Kraji Vysočina kopíruje vývoj v celé České republice, kdy je podle informací Policie ČR[2] kyberkriminalita jediným druhem kriminality, která neustále narůstá.



V roce 2021 řešilo Krajské ředitelství policie kraje Vysočina[3] 386 případů kybernetické kriminality. Což je více jak 8% všech trestných činů spáchaných v Kraji Vysočina. Za posledních několik let je zde patrný výrazný nárůst tohoto druhu kriminality, když v roce 2017 představoval tento druh kriminality jen necelých 5% všech trestných činů spáchaných v Kraji Vysočina. Největší počet případů 199, se týkalo majetkové trestné činnosti. Jde o nejrůznější formy internetových podvodů a protiprávních jednání spáchaných za využití sociálních sítí s cílem neoprávněně se obohatit. Další případy se týkají hospodářské trestné činnosti (113 případů), mravnostní kriminality (44 případů), ale také násilné kriminality (14 případů) a oblasti nehmotných práv. Výrazný nárůst je patrný u majetkové a hospodářské trestné činnosti.

Druhy trestné činnosti páchané v oblasti kybernetické kriminality dokumentované na Krajském ředitelství policie Kraje Vysočina v letech 2017 - 2021

	2017	2018	2019	2020	2021
násilná trestná činnost	21	14	11	12	14
mravnost	29	38	43	48	44
majetková trestná činnost	59	100	116	185	199
ostatní a zbývající trestná činnost	28	9	12	17	16
hospodářská trestná činnost	122	82	115	172	113
celkem	**259**	**243**	**297**	**433**	**386**

[2] https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx
[3] https://www.policie.cz/clanek/podvodnici-vyuzivaji-virtualni-prostredi.aspx

Podle informací z Krajského ředitelství policie Kraje Vysočina lze predikovat nárůst kybekriminality i v budoucnu, a to v návaznosti na stále rostoucí význam elektronické komunikace i v rámci běžného života občanů a stále s rostoucí tzv. „elektronickou gramotností" větší části obyvatelstva, tedy jak pachatelů, tak i poškozených.

V roce 2018 proběhl v Kraji Vysočina mezi žáky na druhém stupni základních škol výzkum Vnímání kyberkriminality mezi dětmi.[4] Výzkum byl realizován v rámci projektu Kraje pro bezpečný internet. Do výzkum se v Kraji Vysočina zapojilo více jak 8 000 žáků a studentů. Z výzkumu vyplynulo, že téměř všichni žáci druhého stupně základní školy mají účet na sociálních sítích a pohybují se denně v prostředí kyberprostoru. Pouze 5% žáků uvedlo, že nepoužívá žádné sociální sítě. Žáci většinou získávají informace o bezpečném chování na internetu od pedagogů. V rámci otázky, od koho by chtěli získávat informace, bylo nejvíce odpovědí, že od pedagogů, případně pak policistů. Výsledky provedeného výzkumu ukázaly, že žáci mají stále nedostatečné znalosti takřka ve všech oblastech týkajících se rizikového chování na internetu a kyberkriminality. Nejnižší znalost je v oblasti porušování autorských práv, které jako kyberkriminalitu označilo jen necelých 40 %. Z jednotlivých druhů kyberkriminality se nejvíce na internetu žáci dopouštějí, ať již vědomě či nevědomě, různých forem neoprávněného přístupu k informačnímu systému, což je samo o sobě trestným činem.

V roce 2020 byl v Kraji Vysočina zpracován Průzkum veřejného mínění o názorech obyvatel Kraje Vysočina na kriminalitu, prevenci kriminality a kyberkriminalitu[5], ve kterém obyvatelé Vysočiny označili kyberkriminalitu, jako druh kriminality, ze které mají největší obavy. Z výsledků dotazování vyplývá:

- nejvíce dotazovaných se setkalo se „spamem" a počítačovým virem. Nárůst lze pozorovat u hoaxu a phisingu.
- zhruba 90 % dotazovaných se obává „zneužití osobních údajů" a počítačových virů
- 60 % dotázaných uvedlo, že se vzdělává v oblasti elektronické bezpečnosti
- 85% dotázaných uvedlo, že seznámilo své děti s nebezpečím používání počítače
- 90% dotázaných používá hesla obsahující minimálně 6 znaků, jednu číslici a malá a velká písmena.
- 90% dotázaných uvedlo, že považují za důležité programy proti kyberkriminalitě

Z průzkumu vyplývá, že uživatelé internetu již nějaké znalosti z oblasti kyberbezpečnosti mají a vzdělávají se v této problematice. Ale stále jsou vzdělávání i jejich znalosti podle respondentů nedostatečné.

Aktivity Kraje Vysočina v oblasti elektronické bezpečnosti v letech 2018 – 2021

Aktivity Kraje Vysočina v oblasti elektronické bezpečnosti byly realizovány na základě Strategie elektronické bezpečnosti Kraje Vysočina 2018 – 2021. Většina aktivit se zaměřovala na podporu prevence a zvyšování povědomí o oblasti kybernetické bezpečnosti. Cílovými skupinami, na které se aktivity pracovní skupiny v tomto období zaměřovaly, byly především děti, rodiče, pedagogové, senioři, odborná veřejnost, dále pak malé a střední firmy.

Veškeré aktivity pracovní skupiny jsou zveřejněny na webových stránkách eBezpečnosti.[6] Na těchto stránkách také funguje informační portál, kde jsou pravidelně zveřejňovány aktuality z oblasti elektronické bezpečnosti pro laiky i pro odborníky (funguje i jako RSS kanál).

[4] https://www.kpbi.cz/prilohy/157_vyzkum_final.pdf
[5] https://www.kr-vysocina.cz/assets/File.ashx?id_org=450008&id_dokumenty=4103882
[6] www.kr-vysocina.cz/ebezpecnost

V roce 2017 došlo k obnovení lektorské skupiny. Jedná se síť lektorů (učitelé, preventisté), kteří jsou schopni školit své kolegy, rodiče, případně studenty v oblasti elektronické bezpečnosti. Lektoři působí pod příspěvkovou organizací Kraje Vysočina Vysočina Education. V rámci lektorské skupiny působilo 6 lektorů a plánuje se její rozšíření, tak, aby minimálně v každém okrese Kraje Vysočina byl jeden proškolený lektor. Semináře probíhaly v letech 2018 až 2021. V letech 2020 a 2021 vzhledem k situaci spojenou epidemií Covid-19 a zavřením škol probíhaly semináře pouze omezeně. Celkem se v rámci Lektorské skupiny uskutečnilo 194 seminářů a proškoleno bylo 4.537 účastníků.

Lektorská skupina 2018 - 2021		
	počet seminářů	**počet proškolených**
2018	50	1366
2019	111	2604
2020	28	501
2021	5	68
CELKEM	**194**	**4537**

Aktivitou zaměřenou na žáky a studenty základních a středních škol v Kraji Vysočina bylo zorganizování kreativních soutěží. Žáci a studenti z Kraje Vysočina mohli vytvářet videa, plakáty, komiksy nebo prezentace. V roce 2018 se jednalo o kreativní soutěž Cloud aneb moje data v internetu. Porota hodnotila 85 soutěžních prací. V roce 2019 byly v rámci soutěže Nezávislí lépe myslí, připraveny soutěžní práce zaměřené na závislost na počítačích, mobilech či internetu. Porota hodnotila cca 80 soutěžních prací. V roce 2020 se jednalo o kreativní soutěž Nevěř všemu na netu. Porota hodnotila 80 soutěžních prací týkajících se pravdivost informací na internetu (fake news, hoaxy, apod.) V roce 2021 byla vyhlášena soutěž týkající se umělé inteligence Ajéje, AI! Kyberbezpečnost z pohledu umělé inteligence. Porota hodnotila cca 100 soutěžních prací.

Pro poskytovatele internetu a firmy zabývající se IT technologiemi v Kraji Vysočina připravila pracovní skupinu značku Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET. V letech 2018 - 2021 značku užívalo sedm firem. Vzhledem ke klesajícímu zájmu o tuto aktivitu se pracovní skupina usnesla značku ke konci roku 2021, po deseti letech, ukončit. Podobnou aktivitu realizovala pracovní skupina pro školy – Značka eBezpečná škola. Značka byla určena pro školy a školská zařízení v Kraji Vysočina, kterým není problematika elektronické bezpečnosti lhostejná. V období 2018 – 2021 značku užívaly 3 školy. Značka vycházela z iniciativy eSafety Label. Vzhledem k tomu, že tato iniciativa byla v roce 2020 ukončena a protože další školy neprojevily o značku zájem, rozhodla se pracovní skupina ke konci roku 2021 značku, po šesti letech, ukončit.

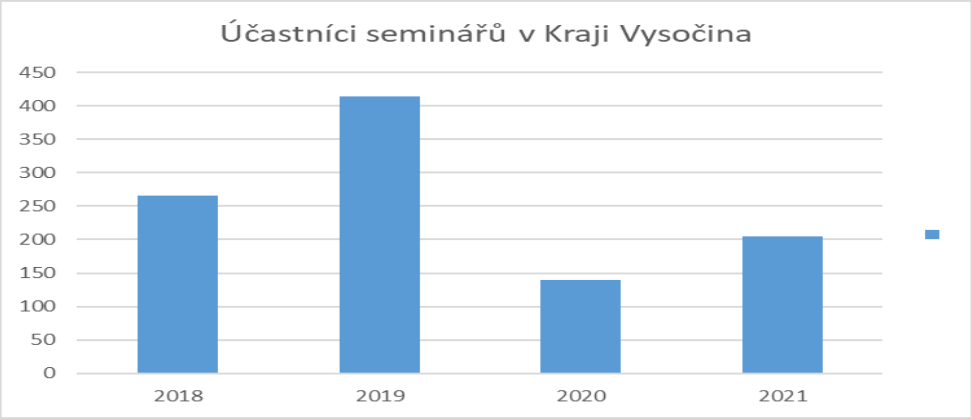
V letech 2020 a 2021 pravidelně také vycházejí každé dva měsíce v Novinách Kraje Vysočina články týkající se elektronické bezpečnosti. Články seznamovali veřejnost s aktuálními hrozbami v této oblasti a možnostmi prevence.

Pracovní skupina zorganizovala velké množství seminářů a školení pro učitele, odborníky, policisty, odbornou veřejnost apod. Každý rok na jaře pořádá pracovní skupina Seminář k problematice el. bezpečnosti. Tento seminář je určen pro zástupce škol, odbornou veřejnost, informatiky obcí a příspěvkových organizací Kraje Vysočina. Ve spolupráci se sdružením CESNET a společnosti AUTOCONT připravila několik školení pro informatiky obcí a příspěvkových organizací v Kraji Vysočina. Každý rok na podzim pořádal Kraj Vysočina ve

spolupráci s Krajským ředitelstvím policie Kraje Vysočina a Policejní akademií mezinárodní konferenci.

Datum	Název semináře	Počet účastníků
15. a 16.2. 2018	Seminář (Ne)bezpečný mobil pro žáky	**80**
14.05.2018	Odborný seminář k problematice elektronické bezpečnosti	**70**
18. a 19. 10. 2018	Mezinárodní konference Řešení elektronického násilí a kyberkriminality	**116**
17.06.2019	Odborný seminář k problematice elektronické bezpečnosti	**68**
17.-18.10.2019	Konference Řešení elektronického násilí a kyberkriminality	**95**
prosinec 2019	Nelegální online obsah - školení pro žáky	**162**
06.12.2019	Nelegální online obsah - školení pro policisty	**25**
17.12.2019	Seminář Kybernetická bezpečnost	**64**
25.06.2020	Seminář k problematice elektronické bezpečnosti (online i prezenčně)	**40**
12.10.2020	Online konference Bezpečné klima na školách	**40**
12.12.2020	Odborný online seminář ke kybernetické bezpečnosti	**60**
31.05.2021	Online seminář k elektronické bezpečnosti	**85**
25.10.2021	Konference Řešení elektronického násilí a kyberkriminality (online i prezenčně)	**95**
02.12.2021	Online seminář na téma mediální gramotnost pro seniory	**25**

Vzhledem k epidemii covid-19 byla realizace prezenčních akcí v letech 2020 - 2021 omezena a často byly akce kombinovány jak prezenčně, tak online. Některé akce se uskutečnili pouze online, jiné byly zrušeny. Obecně je zájem o semináře a konference k problematice el. bezpečnosti vysoký. Co se týče oslovení jednotlivých cílových skupin, největší problém byl s oslovením cílové skupiny rodičů a seniorů.



Iniciativy hSOC, kterou Kraj Vysočina společně inicioval s několika nemocnicemi, se k březnu 2022 účastní již 56 zdravotnických organizací, 8 zřizovatelů, 3 univerzity, 1 ministerstvo a dalších 5 institucí. Aktivity v rámci této komunity zahrnují provoz maillistů včetně systému varování před kybernetickými incidenty a hrozbami, série seminářů, společné zabezpečené sítě hSOC VRF a nově připravovaných sdílených služeb. Více viz https://hsoc.cesnet.cz/

Kraje pro bezpečný internet

Kraj Vysočina je vedoucím krajem projektu Kraje pro bezpečný internet. V roce 2021 bylo do projektu zapojeno aktivně 13 krajů ČR. Projekt je realizován pod záštitou Asociace krajů ČR.

Všechny výstupy projektu jsou dostupné na webových stránkách www.kpbi.cz. V letech 2018 – 2021 vzniklo 40 krátkých videospotů (Rodiče v síti, Pozor na kyberprostor, Internet pod lupou, Internet pod mikroskopem). Dále 18 video tutoriálů zaměřených na IT bezpečnost a 24 pracovních listů. Během tohoto období byly aktualizovány stávající e-learningové lekce a doplněné nové lekce pro žáky a studenty, pro rodiče, pedagogy a soc. pracovníky.

V rámci projektu KPBI byly připraveny e-learningové lekce pro jednotlivé cílové skupiny projektu – děti a studenti, policisté, soc. pracovníci, rodiče a pedagogové.

Každý rok připravuje projekt soutěž pro děti a studenty. Každoročně se do soutěže zaregistruje 30.000 - 35.000 žáků a studentů ze základních a středních škol zapojených do projektu KPBI. V Kraji Vysočina to bylo 3.000 – 4.000 žáků a studentů.

Bezpečnost informací na Krajském úřadě Kraje Vysočina

Činnosti Krajského úřadu Kraje Vysočina v oblasti bezpečnosti lze rozdělit na tzv. vnitřní činnosti směrem dovnitř úřadu a na vnější činnosti, jejichž výstupy jsou primárně cíleny vůči příspěvkovým organizacím, obcím v kraji, veřejnosti a dalším partnerům a subjektům působícím jak v kraji, tak na národní i mezinárodní úrovni.

Vnitřní činnosti jsou zacíleny primárně na zajištění dostatečné úrovně informační a kybernetické bezpečnosti tak, aby byly naplněny požadavky na dostupnost, důvěrnost a integritu informací zpracovávaných krajským úřadem s ohledem na aktuální situace a dobrou praxi, a samozřejmě také tak, aby byly naplněny požadavky zákona č. 181/2018 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů. V rámci těchto vnitřních aktivit lze zmínit např.:

- Neustálé udržování, plánování a zlepšování systému řízení bezpečnosti informací, který je již od roku 2017 certifikován dle mezinárodně uznávané normy ISO/IEC 27001:2013, a to v rozsahu celé organizace, všech zpracovávaných informací a všech informačních aktiv,
- Pravidelné a systematické vzdělávání interních i externích zaměstnanců v oblasti kybernetické bezpečnosti e-learningovou i prezenční formou,
- Pravidelné provádění penetračních testů a posuzování zranitelností technických informačních aktiv i zaměstnanců
- Zavádění moderních technických opatření pro zajišťování informační a kybernetické bezpečnosti,
- Přijímání organizačně procesních opatření pro zajišťování informační a kybernetické bezpečnosti,
- Pravidelná příprava na zajišťování kontinuity poskytovaných služeb a provozovaných systémů, aktualizace a rozvoj disaster recovery plánů,
- a mnoho dalších činností.

Výstupy tzv. vnějších činností jsou zacíleny na příspěvkové organizace, obce, veřejnost, regionální, národní i mezinárodní partnery Kraje Vysočina. V rámci těchto činností provádíme např.:

- informování o aktuálních bezpečnostních hrozbách,
- přijímání, zpracování a další distribuci bezpečnostních hlášení od CSIRT/CERT týmů,
- bezpečnostní monitoring a zajišťování bezpečnosti krajské páteřní sítě Rowanet,
- bezpečné připojení do dalších neveřejných sítí (TESTA-NG, CMS, …),
- poskytování infrastruktury pro bezpečnou archivaci dat,
- osvětovou a vzdělávací činnosti formou seminářů, konferencí, školení, workshopů, apod.,
- zajišťování bezpečného systému pro přeshraniční výměnu zdravotnické dokumentace v rámci členských států EU,
- provoz systému pro detekci kybernetických bezpečnostních událostí v rámci pilotního projektu partnerství s tchaj-wanským CyFoundry (spin-off taipejského Institutu pro informační průmysl, III).

Od roku 2021 je novou významnou aktivitou rovněž příprava Strategie kybernetické bezpečnosti pro organizace zřizované Krajem Vysočina a činnosti vedoucí k opatřením v této strategii definovaným. Rada Kraje RK-10-2021 na svém jednání dne 30. 3. 2021 projednala předloženou Strategii KB pro příspěvkové organizace a usnesením 0548/10/2021/RK uložila všem příspěvkovým organizacím realizovat opatření pro zajištění kybernetické bezpečnosti v souladu s touto Strategií. Strategie KB vychází z materiálu Minimální bezpečnostní standard publikovaného Národním úřadem pro kybernetickou a informační bezpečnost (dále také „NÚKIB“).

III. Cíle a priority kraje v oblasti el. bezpečnosti pro období 2022 – 2025

Cílem Kraje Vysočina jako subjektu veřejné správy je v oblasti elektronické bezpečnosti informování široké veřejnosti o nebezpečí, které hrozí uživatelům informačních a komunikačních technologií, a realizace takových opatření vůči vymezeným cílovým skupinám, která zajistí dostatečnou informovanost uživatelů o rizicích a možnostech ochrany před nimi.

Pracovní skupina se v rámci svých aktivit bude zaměřovat nejen na to, jak uživatele před možnými riziky ochránit, ale také na podporu zavádění procesů zvyšujících kyberbezpečnost. Protože je nezbytné, aby uživatelé nejen věděli, jak se před těmito riziky chránit, ale také to, že oni sami se musí při užívání informačních a komunikačních technologií chovat bezpečně.

Cílové skupiny

- děti a mládež obecně
- učitelé
- domácnosti
- senioři
- odborná veřejnost
- organizace veřejné správy a samosprávy
- malí a střední podnikatelé

Stanovení priorit kraje v oblasti el. bezpečnosti

Pracovní skupina pro elektronickou bezpečnost navrhuje v Kraji Vysočina realizovat následující soubor opatření řešících problematiku elektronické bezpečnosti:

1. Koordinace aktivit a spolupráce s dalšími subjekty

V rámci této priority bude nadále pokračovat práce pracovní skupiny elektronické bezpečnosti, kde se setkávají nejen pracovníci krajského úřadu, ale zástupci dalších subjektů. Bude pokračovat úzká spolupráce se sdružením CESNET, CZ.NIC a CSIRT.CZ při přípravě technických dokumentů a školení. Kraj Vysočina bude také jedním z aktivních členů projektu Kraje pro bezpečný internet, kde dochází k výměně zkušeností v oblasti el. bezpečnosti mezi jednotlivými kraji v České republice a společné koordinaci aktivit v oblasti prevence kyberkriminality. V návaznosti zákon o kybernetické bezpečnosti je pak důležitá spolupráce s národními institucemi jako je NÚKIB a vládní CSIRT. Dále bude realizován návrh na další sdílené kapacity a služby v rámci Asociace krajů ČR (sdílený CSIRT tým, mediátor, auditor kybernetické bezpečnosti, apod.).

2. Vzdělávání v problematice elektronické bezpečnosti

Organizace konferencí, seminářů a školení týkajících se elektronické bezpečnosti pro jednotlivé cílové skupiny. Úzká spolupráce Kraje Vysočina s ostatními členy pracovní skupiny. Spolupráce se školami a školskými zařízeními. Ve spolupráci s Vysočina Education realizace Lektorské skupiny. Organizace soutěží týkající se problematiky bezpečné užívání informačních a komunikačních technologií. Spolupráce s jinými projekty týkajícími se vzdělávání v této oblasti v Kraji Vysočina a ČR.

3. Monitorování, sběr a analýza dat a informací

Sběr a vyhodnocování statistických dat a informací o bezpečnostních incidentech a trestné činnosti. Spolupráce s Policií ČR. Spolupráce s NÚKIB při prevenci kybernetického ohrožení infrastruktury veřejné správy. Spolupráce s CSIRT.CZ a aktivní využívání emergency kanálu hSOC. Využití pravidelných průzkumů veřejného mínění o názorech obyvatel Kraje Vysočina na kriminalitu, prevenci kriminality a kyberkriminalitu.

4. Propagace a medializace

Šíření osvěty a prevence. Zvyšování povědomí cílových skupin o rizicích, nebezpečí a nákladech vyplývajících z elektronické kriminality. Pravidelná aktualizace webových stránek elektronické bezpečnosti a portálu Kam se obrátit s problémy. Pravidelná publikace článků s tématikou el. bezpečnosti pro jednotlivé cílové skupiny v krajských médiích a na webových stránkách. Realizace propagační kampaně k problematice elektronické bezpečnosti. Využívání sociálních sítí a moderních komunikačních prostředků k naplnění této priority. Podpora malých a středních firem a zvyšování povědomí o kyberbezpečnosti v této cílové skupině.

5. Elektronická bezpečnost subjektů veřejné správy

Kraj Vysočina by měl být lídrem aktivit v oblasti zlepšení bezpečnostních standardů a opatření mezi organizacemi veřejné správy působícími na území kraje. Jde zejména o bezpečnost systémů krajského úřadu a příspěvkových organizací kraje se zaměřením na stabilitu, dostupnost a bezpečnost poskytovaných veřejných služeb, ochranu dat a veřejného majetku. Možnost vzniku systému standardů k elektronické bezpečnosti pro organizace zřizované Krajem Vysočina, včetně minimálního standardu ochranných opatření a bezpečnosti dat v souvislosti s ochranou osobních údajů a jiných důležitých informací. Pokračování spolupráce v rámci iniciativy hSOC.

6. Získání finančních prostředků na zajištění základních kroků strategie a případný rozvoj problematiky elektronické bezpečnosti v regionu

Pracovní skupina se bude snažit, mimo prostředky rozpočtu Kraje Vysočina, získat na aktivity v oblasti elektronické bezpečnosti finanční prostředky z národních dotačních programů nebo z evropských fondů, případě od sponzorů.

Příloha č. 1 Přehled legislativních předpisů

Základní zákony, které jsou v oblasti informatiky a telekomunikací nejčastěji uplatňovány:

- zákon č. 89/2012 sb. občanský zákoník
- zákon č. 513/1991 Sb., obchodní zákoník
- zákon č. 121/2000 Sb., autorský zákon
- zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- zákon č. 137/1995 Sb., o ochranných známkách
- zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích
- zákon č. 101/2000 Sb., o ochraně osobních údajů
- zákon č. 140/1961 Sb., trestní zákon
- zákon č. 480/2004 Sb., o některých službách informačních společností
- zákon č. 40/1995 Sb., o regulaci reklamy
- zákon č. 227/2000 Sb., o elektronickém podpisu
- zákon č. 106/2000 Sb., o svobodném přístupu k informacím
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- zákon č. 127/2005 Sb., o elektronických komunikacích
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)

Příloha č. 2 Seznam pojmů

Elektronická informační kriminalita – spočívá ve zneužití informačních a komunikačních technologií k páchání trestných činů
Kybernetická kriminalita (kyberkriminalita) – kriminalita, která může být namířena přímo proti počítačům (hardware, software, dat, sítě) nebo v ní vystupuje počítač jako nástroj pro páchání trestného činu
Hacking – proniknutí do počítačového nebo řídícího systému jinou než standardní cestou při obejití nebo prolomení jeho bezpečnostní ochrany
Cracking – prolamování nebo obcházení ochranných prvků elektronických a programových produktů s cílem jejich neoprávněného použití
Phishing - způsob manipulace prostřednictvím falešných e-mailů a www stránek, jehož cílem je přimět majitele bankovního účtu, aby vyzradil své přístupové údaje k účtu
Pharming – manipulativní postupy, jejichž cílem je přimět uživatele ke sdělení svých osobních údajů
Kybergrooming – jednání osoby, která se snaží zmanipulovat vyhlédnutou oběť a donutit ji k osobní schůzce
Stalking – pronásledování, opakované stupňování obtěžování (pokusy o kontaktování osoby prostřednictvím dopisů, e-mailů, telefonů, chatu, skype, ICQ atd.), které může přejít k vyhrůžkám, ničení majetku apod.
Kyberstalking – zneužívání internetu, mobilních telefonů a jiných informačních a komunikačních technologií ke stalkingu
Kyberšikana – šikanování jiné osoby (ubližování, ztrapňování, obtěžování, ohrožování, zastrašování atd.) s využitím internetu, mobilního telefonu a jiných informačních technologií
Sexting – elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem
Happy slapping – nečekané fyzické napadnutí buď mladistvého, nebo dospělého člověka. Komplic agresora celý čin nahrává na mobilní telefon nebo kameru, video je poté umístěno na internetu.
Hoax – poplašná zpráva
Spamming – zasílání nevyžádané elektronické pošty obvykle s reklamním obsahem
Sociální sítě - označení pro informační sítě, které umožňují vytvářet virtuální společenství
Sociální inženýrství – promyšlená manipulace přirozené důvěřivosti člověka
Kybernetické výpalné – trestná činnost založená na strachu z prezentované hrozby průniku do spravovaného nebo vlastního systému s následným zneužitím nebo zničením dat
Sniffing – neoprávněné odposlouchávání komunikace na síti
Warez – moderní počítačové pirátství, které spočívá v prolamování ochranných prvků programových produktů a jejich šíření pomocí www serverů
ISMS – Systém řízení bezpečnosti informací

Další pojmy jsou dostupné ve **Výkladovém slovníku kyberbezpečnosti (NÚKIB)**

Příloha č. 3 Pracovní tým elektronické bezpečnosti

	jméno	organizace
1.	Jan Břížďala	Radní Kraje Vysočina
2.	Ivana Šteklová	OSH KrÚ
3.	Petr Pavlinec	OI KrÚ
4.	Lucie Časarová	OI KrÚ
5.	Klára Jiráková	OI KrÚ
6.	Dominik Marek	OA KrÚ
7.	Miroslav Jaroš	OA KrÚ
8.	Josef Pokorný/ Andrea Pohanová	OSH KrÚ
9.	Jiří Kafka	OSV KrÚ
10.	Petr Horký	OŠMS KrÚ
11.	Martin Vaněček	Policie ČR
12.	Stanislav Piskač	KHK Jihlava
13.	Andrea Kropáčová	CESNET z.s.p.o.
14.	Jaroslav Dvořák	AUTOCONT a.s.
15.	Roman Křivánek	Vysočina Education
16.	Milena Dolejská	Vysočina Education
17.	Lukáš Habich	Policejní akademie