

**Strategie Kraje Vysočina v
oblasti prevence kybernetické
kriminality
2026 - 2029**

Obsah

Úvod.....	3
I. Úloha a postavení Kraje Vysočina v problematice el. bezpečnosti	4
II. Analýza stavu elektronické bezpečnosti v Kraji Vysočina 2022 – 2025	5
Aktivity Kraje Vysočina v oblasti elektronické bezpečnosti v letech 2022 – 2025.....	6
III. Cíle a priority kraje v oblasti el. bezpečnosti pro období 2026 – 2029.....	11
Cílové skupiny	11
Stanovení priorit kraje v oblasti el. bezpečnosti	11
Příloha č. 1 Přehled legislativních předpisů.....	13
Příloha č. 2 Seznam pojmů	14
Příloha č. 3 Pracovní tým elektronické bezpečnosti	15

Úvod

Strategie Kraje Vysočina v oblasti prevence kybernetické kriminality 2026 - 2029 (dále jen Strategie) je jedním z dokumentů Kraje Vysočina reagující na vzrůstající význam problematiky kyberbezpečnosti a kybernetické kriminality. Dokument představuje cíle a oblasti, které by měly vést ke zlepšení kyberbezpečnosti a prevenci kybernetické kriminality 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 kyberbezpečnosti a prevence kybernetické kriminality. Navazuje na Strategii elektronické bezpečnosti Kraje Vysočina 2022 – 2025. Strategie je vytvořena jako základní koncept aktivit pracovní skupiny elektronické bezpečnosti (dále jen pracovní skupiny) pro roky 2026 – 2029,¹ která na Krajském úřadě Kraje Vysočina působí již od roku 2010. Tato Strategie by také měla sloužit jako základní dokument pro tvorbu dalších koncepčních materiálů týkajících se problematiky IT, kyberbezpečnosti a prevenci kybernetické kriminality.

Strategie je v souladu se základními dokumenty týkajícími se prevence kriminality a kybernetické kriminality v České republice. Jedná se o následující dokumenty - Strategie prevence kriminality v České republice 2022 - 2027, Národní strategie kybernetické bezpečnosti České republiky 2026, Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2026 – 2030. Strategie vychází také z Koncepce prevence kriminality Kraje Vysočina na léta 2023 - 2027, 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 kyberbezpečnosti a rekapituluje aktivity pracovní skupiny v období 2022 – 2025. Druhá část se zabývá analýzou problematiky kybernetické kriminality v Kraji Vysočina a dosavadními aktivitami Kraje Vysočina v této oblasti. Třetí část přináší cíle a jednotlivé priority a aktivity v oblasti kyberbezpečnosti a prevence kybernetické kriminality v Kraji Vysočina na období 2026 - 2029.

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 hejtmána jsou jejím členy zástupci Policie ČR, krajské hospodářské komory, Vysočina Education (příspěvkové organizace Kraje Vysočina) či společnosti Aricoma. 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 číhající 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 má pak bezesporu smysl i na regionální úrovni řešit 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. V roce 2021 byla vytvořena 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 kyberbezpečnosti 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 všech krajů ČR podporovat prevenci a vzdělávání v oblasti kyberbezpečnosti. Od roku 2016 je Kraj Vysočina vedoucím krajem tohoto 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 společného 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 2022 – 2025

Situace v oblasti elektronické bezpečnosti v Kraji Vysočina kopíruje vývoj v celé České republice, kdy je podle informací Policie ČR² kyberkriminalita až do roku 2023 narůstala. V roce 2024 došlo k mírnému poklesu kybernetické kriminality a ostatní kriminality páchaná v kyberprostoru.



V roce 2021 bylo zdokumentováno 386 případů trestných činů s prvky kybernetické kriminality. Tento rok byl ovlivněn covidovými opatřeními a podíl trestné činnosti páchané v kyberprostoru na celkové kriminalitě byl nízký. V roce 2022 šlo o výrazný nárůst kybernetické kriminality v Kraji Vysočina – 722 případů³. Největší počet případů internetové kriminality – celkem 529⁴ - se týkalo majetkové trestné činnosti. Jednalo o nejrůznější formy internetových podvodů a protiprávních jednání spáchaných za využití sociálních sítí s cílem neoprávněně se obohatit za využití různých legend. V roce 2023 byl patrný stále trend narůstající kybernetické kriminality. Celkem se jednalo o 865 případů, opět převažovaly majetkové trestné činy. V roce 2024 byl sledován mírný pokles oproti 2023, přesto se jednalo o vysoký podíl – 790 případů, což bylo cca

² <https://policie.gov.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2024.aspx>

³ <https://policie.gov.cz/clanek/kriminalita-v-kraji-vysocina-v-roce-2022.aspx>

⁴ <https://policie.gov.cz/clanek/vyvoj-kriminality-na-vysocine-v-roce-2023.aspx>

15,3% z celkového počtu trestných činů v Kraji Vysočina. V roce 2024 pachatelé internetové kriminality způsobili škodu ve výši 144 912 162 Kč. Největší podíl tvořily majetkové internetové podvody (inzertní podvody, podvody přes sociální sítě, investiční podvody, social engineering).

V rámci kybernetické kriminality převládají tedy majetkové podvody zaměřené na finanční obohacení pachatelů. Rozsah škod v korunách roste rychleji než počet případů — útoky jsou sofistikovanější a často mají větší finanční dopad. Objasněnost případů zůstává nízká a to z důvodů anonymity, přeshraniční složitosti, využití šifrovacích a anonymizačních nástrojů, apod.. 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. Lze předpokládat, že s rostoucím vlivem AI budou útoky také stále sofistikovanější.

V roce 2023 proběhl v Kraji Vysočina mezi žáky na druhém stupni základních škol Výzkum vnímání kyberkriminality mezi dětmi⁵. Výzkum byl realizován v rámci projektu Kraje pro bezpečný internet. Do výzkumu se v Kraji Vysočina zapojilo více jak 8 500 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 1% 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 často umí rozpoznat ty „klasičtější“ a jasné formy kybernetického nebezpečí (např. phishing, neoprávněné přístupy) — kolem 85 % označilo například e-mail vypadající jako od banky nebo falešnou přihlašovací stránku jako kyberkriminalitu. Naopak nižší znalost je u oblastí týkajících se porušování autorských práv, např. stahování/zpřístupňování filmů či písniček. Jen přibližně 34 % žáků označilo stahování filmu/písničky z internetu a následné sdílení s kamarády za kyberkriminalitu. 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.

Aktivity Kraje Vysočina v oblasti elektronické bezpečnosti v letech 2022 – 2025

Aktivity Kraje Vysočina v oblasti kyberbezpečnosti byly realizovány na základě Strategie elektronické bezpečnosti Kraje Vysočina 2022 – 2025. Většina aktivit se zaměřovala na podporu prevence a zvyšování povědomí o oblasti kybernetické bezpečnosti a prevence kybernetické kriminality. 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).

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. Semináře probíhaly v letech 2022 – 2025 a je o ně stále

⁵ https://kr-vysocina.cz/assets/File.ashx?id_org=450008&id_dokumenty=4124695

⁶ <https://www.kr-vysocina.cz/ebezpecnost>

velký zájem ze strany škol. Celkem se v rámci Lektorské skupiny uskutečnilo 280 seminářů a proškoleny byly 4176 účastníků.

LEKTORSKÁ SKUPINA 2021 - 2025		
	počet seminářů	počet proškolených osob
2022	74	1018
2023	84	1083
2024	92	1697
2025	49	625
	280	4176

Aktivitou zaměřenou na žáky a studenty základních a středních škol v Kraji Vysočina bylo zorganizování kreativních soutěží S Vysočinou bezpečně na internetu. Žáci a studenti z Kraje Vysočina mohli vytvářet videa, plakáty, komiksy nebo prezentace. V roce 2022 se jednalo o kreativní soutěž k tématu "Digitální stopa, aneb víme, co vše o sobě zanecháváme na internetu?" Porota hodnotila 155 soutěžních prací, do soutěže se zapojilo více jak 300 žáků a studentů. V roce 2023 byly v rámci soutěže Jak si ochránit svoji identitu a peníze?, připraveny soutěžní práce zaměřené na digitální identitu a rizika s ní spojená. Porota hodnotila cca 130 soutěžních prací. V roce 2024 se jednalo o kreativní soutěž "Jak nás ovlivňují dezinformace?" Porota hodnotila 143 soutěžních prací týkajících se pravdivosti informací na internetu (fake news, hoaxy, apod.) V roce 2025 byla vyhlášena soutěž "Jak dostat malé děti bezpečně do kybersvěta?". Vyhlášení výsledků soutěže je naplánováno na květen 2026.

V roce 2023 se uskutečnila na Krajském úřadě Kraje Vysočina výstava soutěžních prací kreativní soutěže S Vysočinou bezpečně na internetu. Byly vystaveny vítězné soutěžní práce z ročníků 2011 – 2022.

V letech 2022 a 2025 nepravidelně také vycházely každé dva měsíce v Novinách Kraje Vysočina články týkající se kybernetické bezpečnosti a prevence kybernetické kriminality. 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 vzdělávacími organizacemi připravila několik školení pro informatiky obcí a příspěvkových organizací v Kraji Vysočina. V roce 2022 pořádal Kraj Vysočina v Telči mezinárodní konferenci Digital Partnership for Cybersecurity and Resilience of the Regions. V roce 2023 se na Krajském úřadě Kraje Vysočina uskutečnila konference KPBI Kyberbezpečnost – prevence, osvěta a vzdělávání.

Datum	Název semináře	Počet účastníků
14. 9. 2022	Odborný seminář ke kybernetické bezpečnosti	53
5. – 7. 10. 2022	Mezinárodní konference Digital Partnership for Cybersecurity and Resilience in Regions	150
28. 11. 2022	Odborný seminář Disaster recovery plány a testování kontinuity	31
13. 3. 2023	Workshop k problematice užívání informačních technologií dětmi v ústavních zařízeních	40
20. 6. 2023	Odborný seminář k elektronické bezpečnosti	70

2. 11. 2023	Konference Kyberbezpečnost - prevence, vzdělávání a osvěta	109
2. 6. 2024	Odborný seminář k elektronické bezpečnosti	85
25. 9. 2024	Školení Bezpečnost webových aplikací	14
27.11.2024	Školení E-mailová autentizace	14
2. 6. 2025	Odborný seminář k elektronické bezpečnosti	73
8. 9. 2025	Svět za zrcadlem - pro zaměstnance KrÚ	103
8. 9. 2025	Svět za zrcadlem - pro veřejnost	80
11.9.2025	Webinář pro pedagogy na 1. stupni základních škol	30

Iniciativa hSOC

Iniciativa hSOC, kterou Kraj Vysočina společně inicioval s několika nemocnicemi, se k březnu 2022 zúčastnilo již 56 zdravotnických organizací, 8 zřizovatelů, 3 univerzity, 1 ministerstvo a dalších 5 institucí. Aktivita 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 2024 se do projektu zapojilo aktivně všech 14 krajů ČR. Jako poslední se v roce 2023 připojil Olomoucký kraj. Projekt je realizován pod záštitou Asociace krajů ČR.

Všechny výstupy projektu jsou dostupné na webových stránkách www.kpbi.cz. V letech 2022 – 2025 vznikly v rámci projektu videospoty, nové e-learningové lekce a pracovní listy. Během tohoto období byly aktualizovány stávající e-learningové lekce a doplněné nové lekce pro žáky a studenty, pro rodiče, pedagogy a soc. pracovníky. Nově byly připraveny podcasty Pozor na kyberprostor, Jedná se o 20 dílů rozhovorů s odborníky na kyberbezpečnost.

Každý rok také v rámci projektu KPBI probíhají prezenční semináře a konference zaměřené na vzdělávání žáků a studentů, pedagogů a široké veřejnosti v oblasti kyberbezpečnosti a prevence kyberkriminality.

Každý rok připravuje projekt znalostní kvíz pro děti a studenty, kde si soutěžící mohou ověřit své znalosti z oblasti kyberbezpečnosti a prevence kyberkriminality. Soutěžit mohou žáci 1. a 2. stupně základních škol a studenti středních škol. Každoročně se do soutěže zaregistruje více jak 50.000 žáků a studentů ze základních a středních škol z celé ČR. 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. a nově zákona č. 264/2025 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, a to v rozsahu celé organizace, všech zpracovávaných informací a všech informačních aktiv; v roce 2025 došlo k přechodu na novou verzi normy ČSN EN ISO/IEC 27001:2022,
- 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,
- poskytování konzultačních služeb v oblasti kybernetické bezpečnosti pro příspěvkové organizace zřizované krajem, a to včetně metodické pomoci s řízením informačních aktiv a rizik informační bezpečnosti,
- přijímání, zpracování a další distribuci bezpečnostních hlášení od CSIRT/CERT týmů,
- bezpečnostní monitoring a zajišťování bezpečnosti krajské páteří 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 školicího nástroje Phishingator pro vytváření a správu podvodných phishingových kampaní za účelem praktického školení a tréninku zaměstnanců krajem zřizovaných organizací.

Strategie kybernetické bezpečnosti pro příspěvkové organizace zřizované Krajem Vysočina

Rada Kraje Vysočina schválila strategii kybernetické bezpečnosti pro příspěvkové organizace v březnu 2021. Cílem této strategie je implementace minimálního bezpečnostního standardu vydaného Národním úřadem pro kybernetickou a informační bezpečnost u těchto organizací. Díky implementaci strategie jsou u všech organizací kraje nastavena jednotná pravidla v oblasti bezpečnosti informací a kybernetické bezpečnosti. Výjimky tvoří organizace, které spadají pod zákon o kybernetické bezpečnosti (3 organizace) nebo řídí bezpečnost informací v souladu s mezinárodní normou ČSN/ISO IEC 27001 (1 organizace).

V přípravné části implementace strategie, cca do konce roku 2021, byla vytvořena jednotná vzorová dokumentace (směrnice a provozní řády), která svým obsahem nastavuje pravidla pro plnění zejména organizačních, ale i technických opatření, daných strategií.

V implementační fázi, která probíhala v letech 2022 a 2023, byla u všech organizací provedena identifikace a hodnocení informačních aktiv, hodnocení rizik a tvorba interních předpisů. U všech organizací byl nastaven systém vzdělávání zaměstnanců.

Přehled činností v jednotlivých letech:

Rok 2021:

- Příprava implementace strategie kybernetické bezpečnosti. Vytvoření metodiky a vzorových dokumentů.

Rok 2022:

- Zavedení aplikace na Portálu PO pro jednotnou správu informačních aktiv a rizik. Jednání proběhla u 64 organizací.

Rok 2023:

- Ukončení prvotních jednání, dokončení identifikace aktiv a hodnocení rizik. Zahájení poskytování ICT služeb specialisty Projektové kanceláře Kraje Vysočina.

Rok 2024:

- Implementace organizačních opatření v 87 organizacích Kraje Vysočina. Nemocnice Jihlava a ZZS Kraje Vysočina dosáhly standardů ISO 27001.
- Tyto aktivity řídí Oddělení kybernetické bezpečnosti Odboru analýz a podpory řízení Krajského úřadu Kraje Vysočina.

Další aktivity v roce 2024:

- Phishingator: Nástroj pro vzdělávací phishingové kampaně zaměřené na odhalování bezpečnostních rizik u zaměstnanců. Proběhlo šest kampaní pro různé typy organizací.
- Technická opatření: Spolupráce s Projektovou kanceláří na zlepšení ICT infrastruktury u menších organizací. Aktivity zahrnovaly analýzu stavu ICT, návrh a implementaci nápravných opatření.
- Sdílené služby: Implementace sdílené emailové služby IceWarp, která zajišťuje bezpečnou komunikaci v technologickém centru kraje.

Spolupráce krajského úřadu s obcemi Kraje Vysočina

Nový zákon o kybernetické bezpečnosti se bude vztahovat i na obce s rozšířenou působností (ORP). Obce budou spadat do kategorie povinných subjektů s nižšími povinnostmi a v souvislosti s tím vedení obce bude muset jmenovat osobu odpovědnou za kybernetickou bezpečnost. Kraj Vysočina nabízí pro zájemce z řad ORP pomoc při hledání poskytovatelů této formou společného postupu při administraci zakázky na výběr této služby.

III. Cíle a priority kraje v oblasti el. bezpečnosti pro období 2026 – 2029

Cílem Kraje Vysočina jako subjektu veřejné správy je v oblasti kybernetické bezpečnosti a prevence kybernetické kriminality 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
- rodiče
- 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 na 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.). Krajský úřad se bude v rámci svých možností aktivně účastnit cvičení organizovaných EU organizací ENISA. Koordinace postupu prevence podvodného jednání v online prostředí s dalšími subjekty.

2. Vzdělávání v problematice elektronické bezpečnosti

Organizace konferencí, seminářů a školení týkajících se kyberbezpečnosti a prevence kyberkriminality 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 školení lektorské skupiny. Organizace soutěží týkající se problematiky bezpečného používání informačních a komunikačních technologií. Spolupráce s jinými projekty týkající se vzdělávání v této oblasti v Kraji

Vysočina a ČR. Podpora projektů v oblasti kybernetické bezpečnosti v nově založeném regionálním vzdělávacím subjektu ITNeškola z.s.

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. Monitoring legislativních změn v této oblasti.

4. Propagace a medializace

Šíření osvěty a prevence. Zvyšování povědomí cílových skupin o rizicích, nebezpečí a nákladech vyplývajících z kybernetické kriminality. Pravidelná aktualizace webových stránek Kraje Vysočina zaměřených na kyberbezpečnost. Pravidelná publikace článků s tematikou kybernetické bezpečnosti a prevence kybernetické kriminality 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.

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, příspěvkových organizací kraje, měst a obcí se zaměřením na stabilitu, dostupnost a bezpečnost poskytovaných veřejných služeb, ochranu dat a veřejného majetku. Možnost vzniku systému standardů a doporučení 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, případně 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. 121/2000 Sb., autorský zákon
- zákon č. 137/1995 Sb., o ochranných známkách
- zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Zákon č. 40/2009 Sb., trestní zákoník
- zákon č. 480/2004 Sb., o některých službách informačních společností
- zákon č. 40/1995 Sb., o regulaci reklamy
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- 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. 264/2025 Sb., o kybernetické bezpečnosti
- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (tzv. směrnice NIS2)

Příloha č. 2 Seznam pojmů

Antivir - program, který chrání počítač nebo mobil před škodlivým softwarem (např. viry).

Cloud - online úložiště dat (např. Google Drive, iCloud), které je potřeba také chránit.

Deepfake - uměle vytvořený video nebo audio obsah, který vypadá skutečně, ale je falešný.

Digitální stopa - vše, co o sobě zanecháte na internetu (fotky, komentáře, lajky, historie vyhledávání).

Dvoufázové ověření (2FA) - přihlašování, které kromě hesla vyžaduje i druhý krok (např. kód z SMS).

Etický hacking - legální testování zabezpečení systému, aby se našly slabiny dříve, než je zneužijí zločinci.

Fake news (dezinformace) - nepravdivé nebo záměrně zkreslené informace šířené online.

Firewall (brána) - digitální zeď mezi vaším zařízením a internetem, která blokuje nebezpečné přístupy.

Hacker - Člověk, který proniká do počítačových systémů. Může být zlý („black hat“), ale i etický („white hat“).

Identita online - To, jak se prezentujete na internetu – vaše účty, profilové fotky, komentáře apod.

Krádež identity - Když někdo zneužije vaše údaje k tomu, aby se za vás vydával.

Kyberbezpečnost - Ochrana počítačů, mobilů a dat před útoky, zneužitím nebo poškozením.

Kybergrooming - Navazování kontaktu s dítětem dospělým v online prostoru s cílem ho později zneužít.

Kyberkriminalita - Zločiny, které se dějí v kyberprostoru, například podvody, krádeže dat nebo šíření virů.

Kyberprostor - Virtuální prostředí internetu a všech digitálních sítí, kde komunikujeme, nakupujeme nebo sdílíme informace.

Kyberšikana - ubližování druhým prostřednictvím internetu, např. nadávkami, ponižováním nebo zveřejněním nevhodných fotek.

Malware - škodlivý software, který může krást data, ničit soubory nebo sledovat, co děláte.

Osobní údaje - informace, podle kterých vás lze poznat (např. jméno, adresa, e-mail, rodné číslo).

Penetrační test - zkouška bezpečnosti systému napodobující útok hackera, aby se odhalily slabiny.

Phishing - pokus vylákat vaše údaje pomocí falešných e-mailů nebo webů.

Ransomware - typ malwaru, který uzamkne vaše soubory a požaduje výkupné za jejich odemčení.

Sexting - sdílení intimních fotek nebo zpráv; pokud se dostanou do cizích rukou, mohou být zneužity.

Sociální inženýrství - manipulace lidí, aby sami prozradili důležité informace (např. pod záminkou pomoci).

Spyware - program, který vás tajně sleduje a posílá útočníkovi informace o vaší aktivitě.

VPN (virtuální privátní síť) - nástroj, který šifruje vaši internetovou komunikaci a zvyšuje anonymitu.

Další pojmy jsou dostupné ve [Výkladovém slovníku kyberbezpečnosti \(NÚKIB\)](#)

Příloha č. 3 Pracovní tým elektronické bezpečnosti

	jméno	organizace
1.	Jiří Běhounek	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	OAPŘ KrÚ
7.	Miroslav Jaroš	OAPŘ KrÚ
8.	Jaroslav Nulíček	OSH KrÚ
9.	Andrea Pohanová	OSH KrÚ
10.	Jiří Kafka	OSV KrÚ
11.	Petr Horký	OŠMS KrÚ
12.	Martin Vaněček	Policie ČR
13.	Stanislav Piskač	KHK Jihlava
14.	Andrea Kropáčová	CESNET z.s.p.o.
15.	Jaroslav Dvořák	Aricoma
16.	Roman Křivánek	Vysočina Education
17.	David Průša	Vysočina Education
18.	Pavel Řehoř	Náměstek hejtmána Kraje Vysočina
19.	Jiří Horký	Radní Kraje Vysočina