Strategie elektronické bezpečnosti

Kraje Vysočina

2018 - 2021

Verze 1.1

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 2018 – 2021 (dále jen Strategie) je jedním z kroků Kraje Vysočina jako reakce na vzrůstající význam problematiky elektronické bezpečnosti. Dokument přichází s cíli a oblastmi, které by měly vést ke zlepšení elektronické bezpečnosti nejen dětí a studentů, běžných uživatelů internetu, rodičů apod. z Kraje Vysočina, ale i malých a středních firem, které v Kraji Vysočina působí.

Tento dokument obsahuje strategické záměry Kraje Vysočina ve věcech problematiky elektronické bezpečnosti. Navazuje na Strategii elektronické bezpečnosti Kraje Vysočina 2014 – 2017. Strategie byla vytvořena jako základní koncept aktivit pracovní skupiny elektronické bezpečnosti (dále jen pracovní skupiny) pro roky 2018 – 2021.[1] Také by měla sloužit jako základní dokument pro tvorbu materiálů týkajících se 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 2016 - 2020, Národní strategie kybernetické bezpečnosti ČR na období let 2015 – 2020, akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2015 – 2020. Strategie vychází také z Koncepce prevence kriminality Kraje Vysočina na léta 2017 až 2020, kde je jedním z cílů omezování kriminality páchané prostřednictvím informačních a komunikačních technologií.

Strategie je rozčleněna do 3 částí. První část popisuje úlohu a postavení Kraje Vysočina v oblasti elektronické bezpečnosti a aktivity pracovní skupiny v období 2014 – 2017. 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 roky 2018 - 2021.

[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 CZ a.s. Dále také zástupci sdružení CESNET, CZ.NIC a Národního centra bezpečnějšího internetu. Tato pracovní skupina se od roku 2010 schází v pravidelných dvouměsíčních intervalech a účastní se i jednotlivých akcí organizovaných krajem v oblasti elektronické bezpečnosti.

Škála nebezpečí číhajících na uživatele internetu a dalších elektronických systémů je velmi široká. 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 priority, 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 a zmapování ekonomických ztrát způsobených elektronickou kriminalitou v soukromém i veřejném sektoru.

Další nepopiratelnou rolí kraje je péče o majetek a poskytované veřejné služby včetně jejich bezpečnosti. V tomto ohledu je pak důležitá práce s příspěvkovými organizacemi v oblasti bezpečnosti IT.

Kraj Vysočina se věnoval problematice elektronické bezpečnosti nejen na krajské úrovni, ale také viděl možnost mezikrajské spolupráce v této oblasti. Proto se Kraj Vysočina v roce 2014 stal jedním z iniciátorů vzniku projektu Kraje pro bezpečný internet a od roku 2016 je vedoucím krajem tohoto projektu.

II. Analýza stavu elektronické bezpečnosti v Kraji Vysočina

Dopady kauz a událostí v oblasti elektronické bezpečnosti lze dělit na dvě základní skupiny. Jde o kauzy řešené na úrovni trestní, případně přestupkového řízení (viz následující informace od Policie ČR) a jevy, které jsou obecné povahy a souvisí s využíváním prostředků IT a společenskými jevy.

V oblasti trestních a přestupkových kauz jde pak zejména o následující druhy internetové (informační) kriminality[2]:

- elektronický obchod, podvody
- elektronická komunikace (e-mail, IRC, ICQ)
- útoky na počítačová data, neoprávněný přístup, manipulace s daty
- výhružky, vydírání a šíření poplašných zpráv v síti Internet
- mravnostní kriminalita v síti Internet

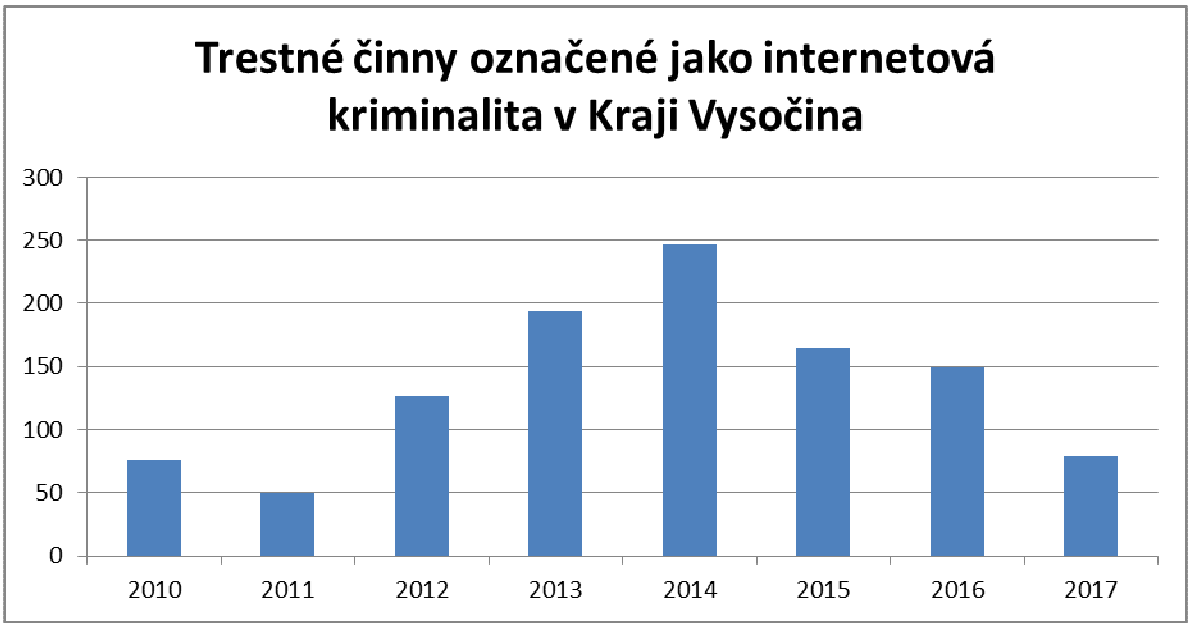
[2] Zdroj: Krajské ředitelství policie Kraje Vysočina: Statistické údaje pro Kraj Vysočina - podklady pro analýzu vývoje kriminality http://www.kr-vysocina.cz/VismoOnline_ActionScripts/File.ashx?id_org=450008&id_dokumenty=4050248

- extrémismus v síti Internet
- monitorování sítě Internet (WWW, FTP, UseNet)
- operativní vyhodnocování dat pomocí specializovaného software
- trestná činnost v souvislosti s porušováním autorských práv v podsítích P2P (DC++, Kazaa aj.)
- porušování duševního vlastnictví neoprávněným užíváním softwaru buď domácím uživatelem, nebo pro komerční účely
- výroba nelegálního softwaru
- neoprávněné užití databází nebo HTML kódu

Statistika trestných činů označených jako internetová kriminalita za období 2014 – 2017 v Kraji Vysočina (zdroj – Krajské ředitelství PČR Jihlava)

	2014	2015	2016	2017 (1-6/2017)
Podvod - prostřednictvím internetové sítě, aukční portály, internetové bazary atd.	176	120	110	57
Pomluva	2	1	4	0
Šíření dětské pornografie, výroba a nakládání s dětskou pornografií	3	5	9	1
Neoprávněný přístup k počítačovému systému a nosiči informací	60	34	22	20
Porušení autorského práva	6	4	4	1
Hanobení národa, rasy, etnické nebo jiné skupiny osob…	0	0	0	0
Celkem	247	164	149	79

Největší množství trestných činů bylo v kategorii podvod prostřednictvím internetové sítě. Jedná se především o nákupy na aukčních portálech, internetových bazarech apod. Dále byl častý trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací, zde byl zaznamenán i vysoký nárůst v počtu trestných činů.



Mezi ostatní druhy jevů, které nejsou vždy nutně řešeny dle trestního a přestupkového práva, patří například[3]:

- Zneužívání sociálních sítí
- Kyberšikana dětí
- Pronásledování kyberstalking
- Kybergrooming
- Sexting
- Happy slapping
- Hoax a spam apod.

K těmto jevům neexistují konkrétní čísla, ale podle odborníků zabývajícími se danou problematikou se tyto jevy vyskytují, a to především mezi mladistvými na školách. Například s kyberšikanou se setkalo 56,53 %[4] českých dětí. Mezi nejčastější formy kyberšikany, jež děti zažívají, patří ubližování v podobě ponižování, urážení a ztrapňování. Nejčastěji byly ke kyberšikaně využity sociální sítě, dále SMS, ICQ a Skype.

V roce 2016 byl v Kraji Vysočina zpracován Průzkum veřejného mínění o názorech obyvatel Kraje Vysočina na kriminalitu, prevenci kriminality a kyberkriminalitu[5]. Z výsledků dotazování vyplývá:

- nejvíce dotazovaných se setkalo se „spamem“ (73,8 %) a počítačovým virem (70,4 %)
- více než 80 % dotazovaných se obává „zneužití osobních údajů“, i když zatím jen každý čtvrtý dotazovaný se s ním setkal
- 57,7 % dotazovaných se obává podvodného prodeje
- nejčastěji používaný způsob zabezpečení počítače je prostřednictvím antivirového programu. Každý druhý dotazovaný používá zaheslování počítače a firewall
- O málo více než polovina (57,7 %) dotazovaných (z těch, kteří mají dítě) seznámil své dítě s nebezpečím v souvislosti s používáním počítače. Jen asi 26 % dotazovaných uvedlo, že ví zcela přesně, co dělá dítě na internetu
- 54,4 % dotazovaných uvádí, že umístilo svoje fotografie na internet
- 19 % dotázaných uvedlo, že používání nelegální software.

Aktivity Kraje Vysočina v oblasti elektronické bezpečnosti v letech 2014 – 2017

Aktivity Kraje Vysočina v oblasti elektronické bezpečnosti byly realizovány na základě Strategie elektronické bezpečnosti Kraje Vysočina 2014 – 2017. Většina aktivit se zaměřovala na podporu prevence a zvyšování povědomí o oblasti elektronické bezpečnosti. Cílovými skupinami, na které se aktivity zaměřovaly, byly především děti, rodiče, učitelé, 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). Kromě webových stránek eBezpečnosti, existuje také portál „Kam se obrátit s problémy s el.

[3] Vysvětlení pojmů viz. Příloha č. 2 – Seznam pojmů
[4] PEDAGOGICKÁ FAKTULTA UNIVERZITA PALACKÉHO V OLOMOUCI: Nebezpečí internetové komunikace III, Olomouc 2012, http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-
[5] https://www.kr-vysocina.cz/assets/File.ashx?id_org=450008&id_dokumenty=4075359
[6] www.kr-vysocina.cz/ebezpecnost

bezpečnosti“. Zde mohou uživatelé najít návod, co dělat a na koho se obrátit, pokud se dostanou do problémů. Je zde také preventivní část, kde je možné získat informace o tom, jak problémům předcházet, a databáze již proběhlých kauz.

Ve spolupráci se sdruženým CESNET došlo k aktualizaci dokumentů Minimálních bezpečnostních standardů. Jedná se o technické dokumenty, které obsahují doporučení, návody a možná opatření k zabezpečení informačních a komunikačních technologií. Aktuálně existují tři dokumenty – pro běžné uživatele, pro středně velké firmy a pro školy a třetí dokument je určen pro malé a střední firmy.

V roce 2017 došlo k obnovení lektorské skupiny, která působila v letech 2010 – 2013. Jedná se síť lektorů (učitelé, preventisté), kteří jsou schopni školit své kolegy v oblasti elektronické bezpečnosti. Na konci roku 2017 byli lektoři proškoleni a samotná školení budou realizována od roku 2018. Lektorská skupina působí pod Vysočina Education.

Aktivitou zaměřenou na žáky a studenty základních a středních škol v Kraji Vysočina bylo zorganizování kreativních soutěží.
V roce 2014 se jednalo o soutěž S Vysočinou bezpečně na internetu. Jednalo se o kombinaci znalostní a kreativní soutěže. V roce 2015 se jednalo o kreativní soutěž s podtitulem „děti učí seniory“ v oblasti el. bezpečnosti. Znalostní soutěž byla realizována v rámci projektu Kraje pro bezpečný internet (viz. info o projektu KPBI). V roce 2016 se jednalo o soutěž ICT nás neděsí aneb bezpečně v kyberprostoru. Porota hodnotila cca 80 soutěžních prací. V roce 2017 představila pracovní skupina kreativní soutěž s názvem Internet věcí, je věcí nás všech, kdy tématem soutěžních příspěvků byl internet věcí a rizika s ním spojená. Porota hodnotila cca 110 soutěžních prací.

Pro malé a střední firmy, které jsou kyberkriminalitou také velmi ohroženy, představila pracovní skupina značku Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET. Jedná se o certifikaci pro IT firmy v Kraji Vysočina, které poskytují služby nebo produkty naplňující myšlenku el. bezpečnosti. Aktuálně značku užívá sedm ICT společností z Kraje Vysočina.

Podobnou aktivitu představila pracovní skupina v roce 2015 pro školy – Značka eBezpečná škola. Tato značka je určena pro školy a školská zařízení v Kraji Vysočina, kterým není problematika elektronické bezpečnosti lhostejná. Školy musí splnit určitá daná kritéria apoté mohou značku po dva roky využívat. Aktuálně užívají značku 3 školy.

Pracovní skupina zorganizovala velké množství seminářů a školení pro učitele, odborníky, policisty, odbornou veřejnost apod. Každý rok v dubnu 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 připravila několik školení pro informatiky obcí a příspěvkových organizací v Kraji Vysočina. Každý rok na podzim pořádá Kraj Vysočina ve spolupráci s Krajským ředitelstvím policie Kraje Vysočina a Policejní akademií připravuje mezinárodní konferenci. Tato konference každý rok naplní kapacitu kongresového sálu Krajského úřadu Kraje Vysočina v Jihlavě.

Datum	Název semináře	Počet účastníků
19. května 2014	Odborný seminář k problematice elektronické bezpečnosti	52
9. a 10. října 2014	Mezinárodní konference – Řešení elektronického násilí a kyberkriminality	110

11. května 2015	Odborný seminář k problematice elektronické bezpečnosti	71
14. prosince 2015	Seminář k bezpečnosti sítí	52
15. a 16. října 2015	Mezinárodní konference – Řešení elektronického násilí a kyberkriminality	110
19. a 20. února 2016	KPBI – Semináře k finanční gramotnosti na internetu	120
31. března 2016	KPBI – Seminář kyberbezpečnost pro informatiky	40
16. května 2016	Odborný seminář k problematice elektronické bezpečnosti	76
13. a 14. října 2016	Mezinárodní konference – Řešení elektronického násilí a kyberkriminality	110
19. dubna 2017	Odborný seminář k problematice elektronické bezpečnosti	77
6. března 2017	Seminář legislativní aspekty monitoringu sítí a směrnice NIS, direktivy GDPR a novelizace ZKB	82
12. června 2017	Seminář GDPR	79
19. a 20. října 2017	Mezinárodní konference – Řešení elektronického násilí a kyberkriminality	110
28. listopadu 2017	KPBI – Školení pro soc. pracovníky k el. bezpečnosti	15
29. listopadu 2017	KPBI - Školení pro pedagogy k el. bezpečnosti	27
14. prosince 2017	KPBI – Školení pro policisty k el. bezpečnosti	21
9. prosince 2017	Školení elektronická bezpečnost – lektorská skupina	9

Obecně se zájem o účast na semináře k problematice el. bezpečnosti zvyšuje. Často poptávka převyšuje kapacitu místností, kde jsou semináře realizovány. Jak je viditelné z grafu níže nárůst počtu účastníků seminářů je v jednotlivých letech plynulý. V roce 2014 to bylo 162 osob, v roce 2017 420 osob. Co se týče oslovení jednotlivých cílových skupin, největší problém byl s oslovením cílové skupiny rodičů a seniorů.

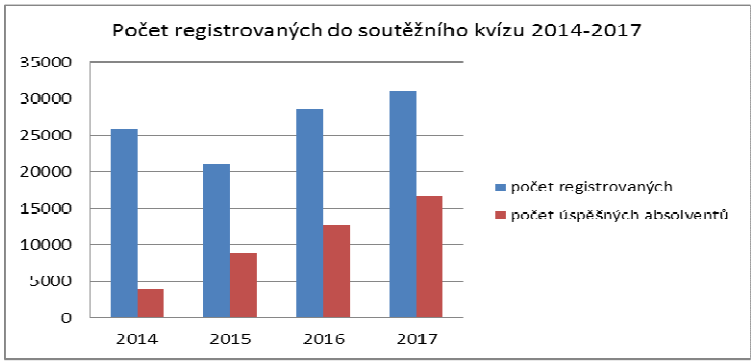
Kraje pro bezpečný internet

Kraj Vysočina byl v roce 2013 jedním z iniciátorů projektu Kraje pro bezpečný internet. V roce 2016 se stal vedoucím krajem projektu. Původní myšlenka sdílení výstupů a aktivit v oblasti el. bezpečnosti v jednotlivých zapojených krajích do projektu se rozšířila na velké množství společných aktivit projektu. V roce 2017 bylo do projektu zapojeno aktivně 12 krajů ČR. Projekt je realizován pod záštitou Asociace krajů ČR.

V rámci projektu vznikly webové stránky www.kpbi.cz, kde jsou dostupné všechny výstupy projektu. V rámci projektu KPBI byly připraveny e-learningové lekce pro jednotlivé cílové skupiny projektu – děti a studenti, policisté, soc. pracovníci, rodiče a pedagogové. Pro cílovou skupinu

senioři a děti a mládež byly představeny krátké videospoty týkající se problematiky el. bezpečnosti.

Každý rok připravuje projekt soutěž pro děti a studenty. V roce 2017 se do soutěže zaregistrovalo přes 31 000 dětí ze zapojených krajů do projektu KPBI, viz graf níže. V Kraji Vysočina to bylo více jak 4 000 registrovaných dětí. Kraj Vysočina pořádal také soutěž škol, kde v letech 2016 a 2017 vyhrálo Gymnázium, Střední odborná škola a Vyšší odborná škola Ledeč nad Sázavou, kde se zaregistrovalo do soutěžního kvízu téměř 70% žáků a studentů.



Bezpečnost informací na Krajském úřadě Kraje Vysočina

Na Krajském úřadě Kraje Vysočina byl v letech 2015 a 2016 implementován systém řízení bezpečnosti informací dle mezinárodně uznávaného standardu ISO/IEC 27001:2013. Od září 2016 do února 2018 probíhal projekt Profesionální a bezpečný úřad, v rámci kterého mimo jiné byl implementovaný systém řízení bezpečnosti informací certifikován podle normy ČSN ISO/IEC 27001:2014. Certifikace proběhla v lednu 2017. Rovněž v rámci tohoto projektu byla uskutečněna tato školení:

- základní vzdělávání – Úvodní školení ISMS – proškoleni všichni zaměstnanci Krajského úřadu Kraje Vysočina
- specializované vzdělávání - Udržení kontinuity organizace – proškoleno 20 osob
- specializované vzdělávání - Procesní řízení informační bezpečnosti - proškoleno 20 osob
- specializované vzdělávání - Řízení rizik informační bezpečnosti - proškoleno 20 osob
- specializované vzdělávání - Interní audit informační bezpečnosti - proškoleno 15 osob

V lednu roku 2018 proběhl první dozorový audit, který v ISMS neshledal významnější problémy či odchylky od normy.

Dále od čtvrtého kvartálu roku 2017 probíhá průběžné vzdělávání všech zaměstnanců zařazených do Krajského úřadu Kraje Vysočina formou e-learningu. Toto školení je zaměřeno na praktická témata z oblastí, jako jsou hrozby na webových stránkách, nebezpečné soubory, sociální inženýrství, phishing podvodné e-maily, šifrování v praxi, bezpečnost hesel apod.

Dále v roce 2017 krajský úřad navázal spolupráci s Krajským ředitelstvím policie kraje Vysočina, která spočívá převážně ve sdílení informací o aktuálních hrozbách v oblasti kybernetické bezpečnosti a v upozorňování na ně subjektům v Kraji Vysočina, jako je veřejnost, příspěvkové organizace Kraje Vysočina a soukromé subjekty. V rámci této spolupráce v roce 2017 vznikly dvě upozornění na hrozby ransomware včetně konkrétních technických doporučení na bezpečnostní opatření a kontroly.

III. Cíle a priority kraje v oblasti el. bezpečnosti pro období 2018 – 2021

Cílem Kraje Vysočina jako subjektu veřejné správy by v oblasti elektronické bezpečnosti mělo být 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 bezpečnost. 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
- školní mládež (základní a střední školy)
- malí a střední podnikatelé
- domácnosti
- senioři
- odborná veřejnost
- organizace veřejné správy

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. V návaznosti na možné přijetí nové legislativy (zákon o kybernetické bezpečnosti) bude pak důležitá spolupráce s národními institucemi jako je NÚKIB a vládní CSIRT.

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. 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 zapojení do systému Warden. K naplnění této priority bude využita nově zřízená pozice bezpečnostního analytika ICT na krajském úřadě.

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 e-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.

5. Podpora drobným a středním podnikatelům

Propagace a rozšiřování značky KRAJ VYSOČINA DOPORUČUJE PRO BEZPEČNÝ INTERNET. Organizace školení a poskytování materiálů této cílové skupině. Příprava projektů zaměřených na vzdělávání v oblasti poskytování bezpečnostních služeb pro domácnosti a malé podniky. Spolupráce s krajskou a okresními hospodářskými komorami.

6. 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.

7. 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

Příloha č. 2 Seznam pojmů

Elektronická informační kriminalita – spočívá ve zneužití informačních a komunikačních technologií k páchání trestných činů
Kybernetická kriminalita (kybernalita) – 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

Příloha č. 3 Pracovní tým elektronické bezpečnosti

	jméno	organizace
1.	Jiří Běhounek	Hejtman Kraje Vysočina
2.	Ivana Šteklová	OSH KrÚ
3.	Petr Pavlinec	OI KrÚ
4.	Lucie Časarová	OI KrÚ
5.	Andrea Pohanová	OSH KrÚ
6.	Ivana Matoušková	OSV KrÚ
7.	Petr Horký	OŠMS KrÚ
8.	Martin Vaněček	Policie ČR
9.	Stanislav Piskač	KHK Jihlava
10.	Andrea Kropáčová	CESNET z.s.p.o.
11.	Zdeněk Záliš	NCBI
12.	Jiří Palyza	NCBI
13.	Jaroslav Dvořák	AutoCont CZ a.s.
14.	Roman Křivánek	Vysočina Education
15.	Milena Dolejská	Vysočina Education
16.	Lukáš Habich	VPŠ Praha – pracoviště Jihlava
17.	Dominik Marek	OA KrÚ
18.	Jiří Průša	CZ.NIC
19.	Věra Mikušová	CZ.NIC