Strategie elektronické bezpečnosti Kraje Vysočina

2014 - 2017

Verze 1.1

Obsah

Úvod

Strategie elektronické bezpečnosti Kraje Vysočina 2014 – 2017 (dále jen Strategie) je jedním z kroků Kraje Vysočina jako reakce na vzrůstající význam problematiky elektronické bezpečnosti. Přichází s aktivitami, které by měly vést ke zlepšení elektronické bezpečnosti nejen dětí, běžných uživatelů internetu, rodičů apod., ale i malých a středních firem, které působí v Kraji Vysočina.

Tento dokument obsahuje strategické záměry Kraje Vysočina ve věcech problematiky elektronické bezpečnosti. Navazuje na Strategii elektronické bezpečnosti Kraje Vysočina 2010 – 2013. Strategie byla vytvořena jako základní koncept aktivit pracovní skupiny elektronické bezpečnosti (dále jen pracovní skupiny) pro roky 2014 – 2017.[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 dva vládní dokumenty - o Strategii prevence kriminality v České republice na léta 2012 až 2015 a o Strategii pro oblasti kybernetické bezpečnosti ČR na období 2012 – 2015. Strategie vychází také z Koncepce prevence kriminality Kraje Vysočina na léta 2013 až 2016, 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 2010 – 2013. 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 2014 - 2017.

[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 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, Vyšší policejní školy v Praze – pracoviště Jihlava, Vysočina Education (příspěvkové organizace Kraje Vysočina) či společnosti AutoCont CZ a.s. Dále také zástupci sdružení CESNET 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.

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
- 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.)

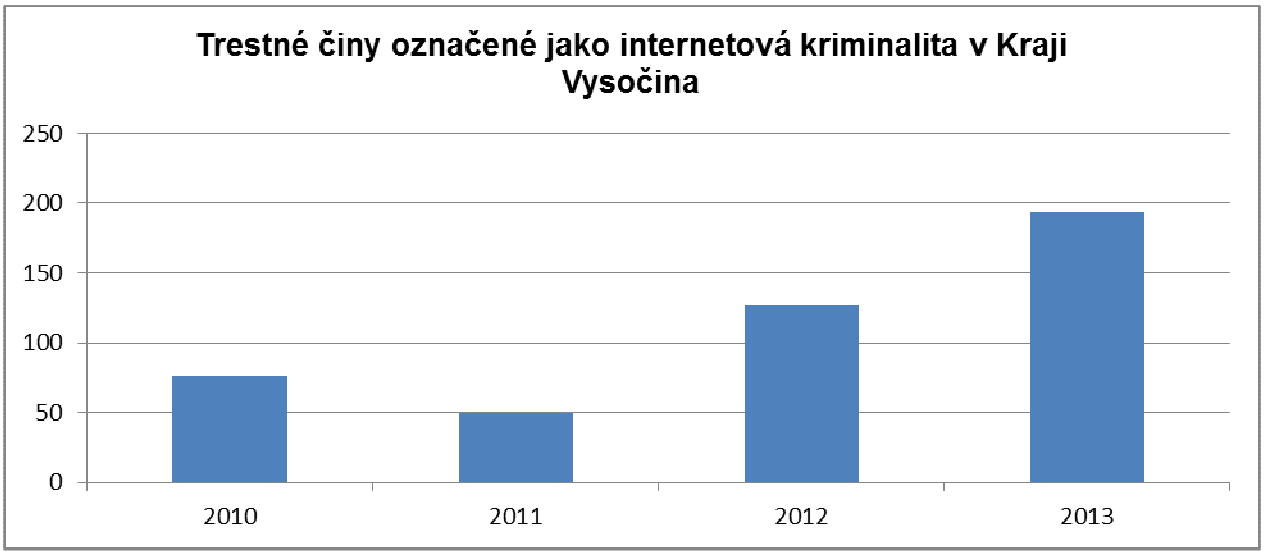
[2] Zdroj: Krajské ředitelství policie Kraje Vysočina: Statistické údaje pro Kraj Vysočina - podklady pro analýzu vývoje kriminality http://www.kr-vysocina.cz/VismoOnline_ActionScripts/File.ashx?id_org=450008&id_dokumenty=4050248

- 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 2010 – 2013 v Kraji Vysočina (zdroj – Krajské ředitelství PČR Jihlava)

	2010	2011	2012	2013
Podvod - prostřednictvím internetové sítě, aukční portály, internetové bazary atd.	61	44	106	155
Pomluva	2	2	5	2
Šíření dětské pornografie, výroba a nakládání s dětskou pornografií	2	1	0	7
Neoprávněný přístup k počítačovému systému a nosiči informací	7	1	7	23
Porušení autorského práva	4	1	9	6
Hanobení národa, rasy, etnické nebo jiné skupiny osob…		1	0	1
Celkem	76	50	127	194

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. Celkem v roce 2013 bylo 155 trestných činů označených jako internetová kriminalita, což je nárůst oproti předchozím rokům.



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.

Aktivity Kraje Vysočina v oblasti elektronické bezpečnosti v letech 2010 – 2013

Se schválením Strategie elektronické bezpečnosti kraje Vysočina 2010 – 2013 začala formálně pracovat Pracovní skupina el. bezpečnosti. Její aktivity se zaměřovaly především na zvyšování povědomí o problematice elektronické bezpečnosti. Cílovými skupinami, na které se aktivity zaměřovaly, byly především děti, rodiče, učitelé, senioři, odborná veřejnost, dále pak malé a střední firmy.

Dále byly vytvořeny webové stránky,[5] kde jsou zveřejňovány kompletní informace o aktivitách Kraje Vysočina v oblasti elektronické bezpečnosti. Kromě webových stránek eBezpečnosti, představila pracovní skupina portál „Kam se obrátit s problémy s el. 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 vznikly dokumenty Minimálních bezpečnostních standardů. Jedná se o technický dokument, který obsahuje doporučení, návody a možná opatření k zabezpečení informačních a komunikačních technologií. V letech 2010 – 2013 vznikly tři dokumenty – pro běžné uživatele, pro středně velké firmy a pro školy a třetí dokument je určen pro malé a střední firmy. V Krajských novinách byly publikovány články týkající se elektronické bezpečnosti. Ve spolupráci s Policií ČR a státním zastupitelstvím byl vytvořen dokument Případy zneužití internetu či počítačových programů v Kraji Vysočina, který obsahuje proběhlé kauzy elektronické kriminality v Kraji Vysočina. Členové pracovní skupiny vytvořili také prezentaci Společně proti kyberšikaně. Jedná se o materiál určený pro školy (učitelé, žáci) obsahující základní informace týkající se el. bezpečnosti a kyberšikany. Materiál také obsahuje návod pro školy, jak řešit kauzy spojené s kyberšikanou, kybergroomingem apod.

Jednou z prvních aktivit pracovní skupiny bylo vytvoření Lektorské skupiny. Jedná se síť lektorů (učitelé, preventisté), kteří jsou schopni školit své kolegy v oblasti elektronické bezpečnosti. Ti

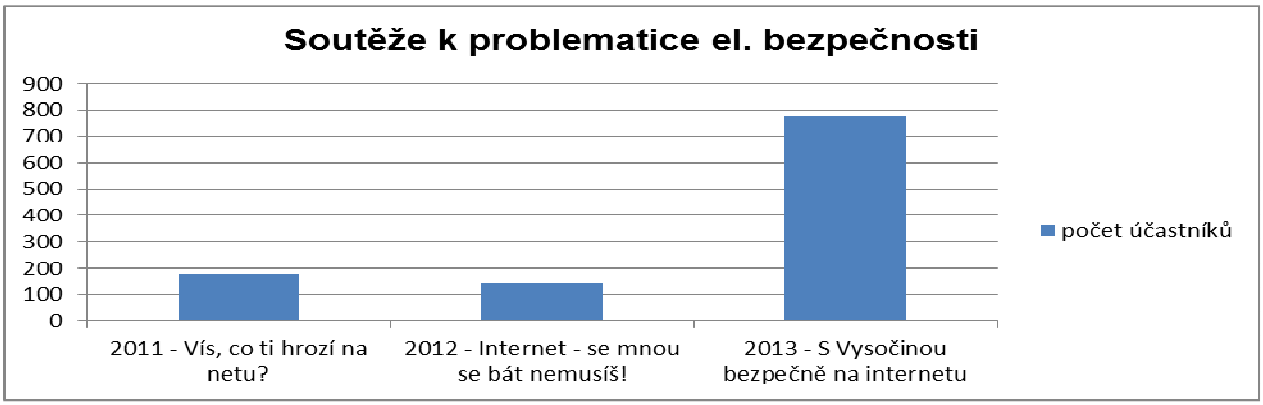
[3] Vysvětlení pojmů viz Příloha č. 2 – Seznam pojmů

[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-

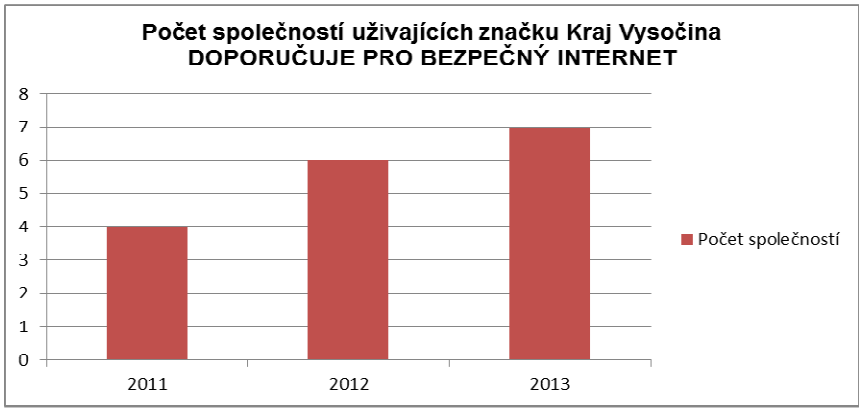
[5] www.kr-vysocina.cz/ebezpecnost

od roku 2010 vyškolili 242 osob a dále také vykonávali metodické konzultace s 9 institucemi (školy, úřady apod.). Tato skupina byla dále rozšířena v rámci projektu i-Bezpečná škola.

Aktivitou zaměřenou na žáky a studenty základních a středních škol v Kraji Vysočina bylo zorganizování soutěží. V roce 2011 se jednalo o soutěže „Víš, co ti hrozí na netu?“, v roce 2012 „Internet – se mnou se bát nemusíš“. Studenti měli za úkol pomocí plakátu, filmu, prezentace apod. zpracovat problematiku elektronické bezpečnosti a kyberšikany. V roce 2013 byla vyhlášena soutěž „S Vysočinou bezpečně na internetu“. Jednalo se o znalostní soutěž pro žáky ZŠ a SŠ.



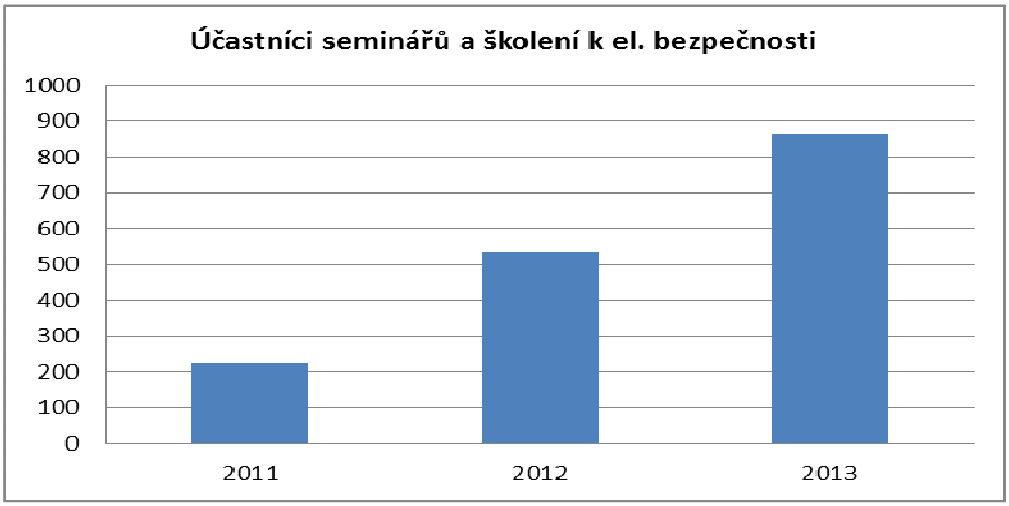
Pro malé a střední firmy, které jsou kyberkriminalitou také velmi ohroženy, představila pracovní skupina značku Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET. Jedná se o certifikaci pro IT firmy v Kraji Vysočina, které poskytují služby nebo produkty naplňující myšlenku el. bezpečnosti. Aktuálně značku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



Pracovní skupina zorganizovala velké množství seminářů a školení pro učitele, odborníky, 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 dvě školení pro informatiky obcí a příspěvkových organizací v Kraji Vysočina. V letech 2011 až 2013 se členové pracovní skupiny podíleli ve spolupráci s Vyšší policejní školou Ministerstva vnitra v Praze – pracoviště Jihlava na pořádání mezinárodní konference týkající se kybernetické kriminality, kyberšikany apod. Zájem o tuto konferenci neustále narůstá, v roce 2011 se jí účastnilo 80 osob, v roce 2013 to bylo 120 osob. Zájemci o tuto konferenci také mohli sledovat online přenos.

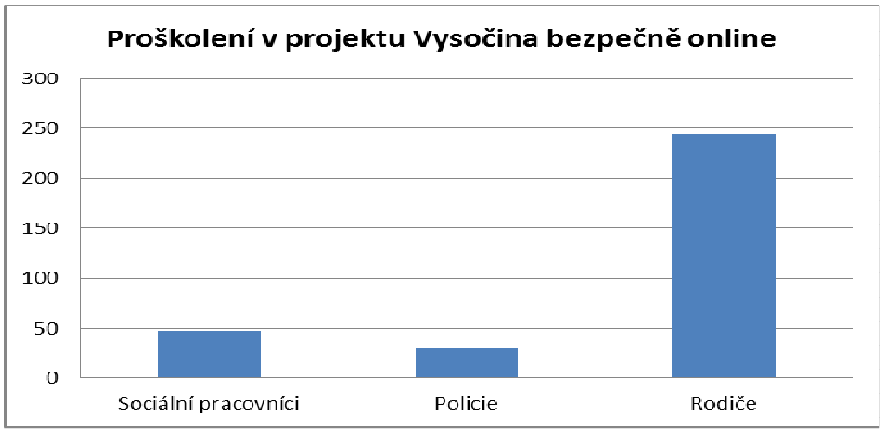
Datum	Název semináře	Počet účastníků
1. 4. 2011	Seminář k problematice elektronické bezpečnosti	39
12. 4. 2011	Školení pro poskytovatele internetového připojení k problematice el. bezpečnosti	25
12. 10. 2011	Prevence rizikového chování dětí a mládeže při užívání informačních a komunikačních technologií na základních a středních školách Kraje Vysočina	38
13.-14. 10. 2011	Dětská kybernetická kriminalita a sociální sítě	80
15. 2. 2012	Školení pro prodejce HW a SW k problematice el. bezpečnosti	17
20. 3. 2012	Seminář CESNET k problematice el. bezpečnosti	48
5. 4. 2012	Seminář k problematice elektronické bezpečnosti	39
11.-12.2012	Konference Eliminace dětské kybernetické kriminality	100
29. 4. 2013	Seminář k problematice el. bezpečnosti	38
1. - 30. 6. 2013	Školení pro sociální pracovníky k problematice el. bezpečnosti	48
19. - 20. 9. 2013	Řešení elektronického násilí a kyberkriminality páchané na dětech a mezi dětmi	120
10. - 12. 2013	Semináře pro rodiče a místní komunity	244
10. - 12. 2013	Školení pro policisty	30
25. 11. 2013	Školení CESNET k problematice el. bezpečnosti	44

Obecně se povědomí o aktivitách Kraje Vysočina a o elektronické bezpečnosti zvyšuje, což je patrné i z počtu účastníků seminářů a školení k problematice el. bezpečnosti. V roce 2011 to bylo více jak 200 účastníků, v roce 2013 se seminářů a školení zúčastnilo přes 800 osob. Tento nárůst byl způsoben nejen vzrůstajícím zájmem o tuto problematiku, ale také realizací projektů Vysočina bezpečně online a i-Bezpečná škola. Co se týče oslovení jednotlivých cílových skupin, největší problém byl s oslovením cílové skupiny rodičů, běžných uživatelů a seniorů.



Kraj Vysočina ve spolupráci s Národním centrem bezpečnějšího internetu realizoval v roce 2013 projekt Vysočina bezpečně online. Jedná se o projektu financovaný z Programu prevence

kriminality Ministerstva vnitra. Součástí projektu je školení pro sociální pracovníky, pro pracovníky místní policie a pro rodiče. V rámci projektu byla také realizována osvětová krajská kampaň. Zástupci pracovní skupiny jsou členy expertní skupiny projektu i-Bezpečná škola, který realizuje Vysočina Education. V rámci tohoto projektu došlo k rozšíření lektorské sítě. Byla zorganizována školení pro učitele, školní preventisty v 10 zapojených školách. Za necelé dva roky realizace tohoto projektu bylo proškoleno 145 osob – pedagogických pracovníků. Kraj Vysočina ve spolupráci s Vysočina Education také realizoval seminář pro studenty týkající se problematiky sociálních sítí (Facebook apod.). Celkem bylo proškoleno 471 studentů.



Pro zpracování této strategie jsou využity zkušenosti britského regionu Wales a jeho eCrime strategie. Kraj Vysočina podepsal memorandum o zapojení do společného projektu s 15 evropskými regiony, které budou usilovat o podporu z evropských fondů. Problematika elektronické bezpečnosti se také stala součástí mezinárodních projektů. Členové pracovní skupiny se stali členy projektu DE-LAN, který měl za úkol zefektivnit práci v pracovní skupině a někteří členové pracovní skupiny měli možnost navštívit britský region Wales a osobně se seznámit s jejich projektem eCrime a vyměnit si s britskými kolegy své zkušenosti s problematikou elektronické bezpečnosti.

Kraj Vysočina byl společně s Plzeňským krajem iniciátorem projektu Kraje pro bezpečný internet. Tento projekt, který byl spuštěn na podzim 2013, je zaměřen na výměnu zkušeností v oblasti el. bezpečnosti mezi jednotlivými kraji v České republice. Dle cílů tohoto projektu bude vytvořena „projektová šablona“ pro jednotlivé kraje, na základě které si každý kraj bude realizovat svůj vlastní projekt.

Krajský úřad Kraje Vysočina se stal také obětí elektronické kriminality. Jednalo se například o zneužití SIM karet v majetku kraje či o zveřejnění licencovaných dat apod. V této souvislosti byly v roce 2010 vytvořeny dokumenty Strategie ICT Kraje Vysočina a Strategie bezpečnosti ICT Kraje Vysočina. Strategie upozorňují na to, že vedle stabilní infrastruktury a jednoduše použitelných aplikací je nutné se soustředit na znalosti skupin uživatelů, bezpečnost systému a předávání informací v rámci celého regionu, nejen krajského úřadu. Jako rizikové oblasti vyhodnotily především dlouhodobě neřešenou problematiku ICT bezpečnosti na úrovni příspěvkových organizací kraje (zejména v oblasti zdravotnictví) či nedostatečné vyhodnocování bezpečnostních incidentů. Na základě těchto dokumentů vznikl na krajském úřadě tým vnitřní bezpečnosti a v roce 2013 byla zřízena pozice bezpečnostního analytika kraje na úseku ICT, který se zabývá mimo jiné administrací a vyhodnocováním výstupů systémů pro sběr a analýzu bezpečnostních incidentů, organizací, popř. realizací preventivních akcí – penetrační testy, bezpečnostní školení a spoluprací s pracovní skupinou eBezpečnost, CSIRT.CZ a NBÚ. Uvedené aktivity jsou realizovány jak vůči infrastruktuře krajského úřadu, tak vůči příspěvkovým organizacím kraje a metodicky i vůči obcím.

III. Cíle a priority kraje v oblasti el. bezpečnosti pro období 2014-2017

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, NIC.CZ 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 NBÚ 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 NBÚ 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.

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

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 řídicího 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

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.	Josef Pokorný	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.	Ivo Kuttelwascher	Vysočina Education
16.	Lukáš Habich	VPŠ Praha – pracoviště Jihlava
17.	Kamil Talavašek	OA KrÚ
18.	Zdeněk Borůvka	SPŠ Třebíč