Kraj Vysočina

Strategie elektronické bezpečnosti kraje Vysočina

2010 - 2013

Verze 1.1

tel.: 564 602 348, fax: 564 602 432, e-mail: posta@kr-vysocina.cz, internet: www.kr-vysocina.cz
IČ: 70890749, bankovní spojení: Volksbank CZ, a.s., č.ú.: 4050005000/6800

Tento dokument obsahuje strategické záměry kraje Vysočina ve věcech problematiky elektronické bezpečnosti. Byl vytvořen jako základní koncept aktivit pracovního týmu elektronické bezpečnosti pro rok 2010 – 2013.

Pracovní tým elektronické bezpečnosti

Zdeněk Ryšavý, radní kraje Vysočina

Ing. Ivana Šteklová, vedoucí odboru sekretariátu hejtmana

Ing. Petr Pavlinec, vedoucí odboru informatiky Krajského úřadu kraje Vysočina

Ing. Josef Pokorný, úředník odboru sekretariátu hejtmana na úseku prevence kriminality Krajského úřadu kraje Vysočina

Mgr. Ivana Matoušková, úředník na úseku sociálně právního poradenství a sociálně právní ochrany odboru sociálních věcí a zdravotnictví Krajského úřadu kraje Vysočina

Mgr. Petr Horký, pracovník oddělení mládeže a sportu odboru školství, mládeže a sportu Krajského úřadu kraje Vysočina.

Mgr. Jitka Fejtlová, státní zástupce Jihlava

Ing. Stanislav Piskač, krajská hospodářská komora

František Pokorný, Policie ČR ředitelství pro kraj Vysočina

Recenzenti

Zástupci sdružení CESNET a pilotního pracoviště CSIRT.CZ

Odbor informatiky KrÚ

Zástupci odborné veřejnosti

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

Pishing - 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 – znamená pronásledování, opakované stupňování obtěžování (pokusy o kontaktování osoby prostřednictvím dopisů, e-mailů, telefonů, chatu, skype, ICQ ad.), 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 ad.) s využitím internetu, mobilního telefonu a jiných informačních technologií

Sexting – elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem

Hoax – poplašná zpráva

Spamming – zasílání nevyžádané elektronické pošty obvykle s reklamním obsahems

Sociální sítě - označení pro informační sítě, které umožňují vytvářet virtuální společen

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

Strategie elektronické bezpečnosti kraje Vysočina

1. Úloha a postaveni kraje Vysočina v problematice e-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 především předcházet těmto rizikům. Proto také byla rozhodnutím vedení kraje 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, státního zastupitelství, hospodářské komory a školských zařízení.

Škála nebezpečí číhajících na uživatele internetu a dalších elektronických systémů je velmi široká. Část této problematiky je zařazena mezi priority mnoha organizací se národní a mezinárodní působností. 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, ale také třeba seniorů, ohrožení malých a středních firem, preventivní akce pro odbornou veřejnost, shromažďování a vyhodnocování statistický dat a zmapování ekonomických ztrát způsobených elektronickou kriminalitou v soukromém i veřejném sektoru.

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.

2. Cíl strategie

Cílem Strategie je informovat o nebezpečí, které hrozí uživatelům informačních a komunikačních technologií a přijmout vůči vymezeným cílovým skupinám taková opatření, která zajistí dostatečnou informovanost uživatelů o rizicích a možnostech ochrany před nimi.

3. Cílové skupiny

- děti a mládež obecně
- školní mládež (základní a střední školy)
- drobní a střední podnikatelé
- domácnosti
- senioři
- odborná veřejnost

4. Analýza stavu elektronické bezpečnosti v kraji Vysočina

V oblasti elektronické bezpečnosti se typicky objevují následující jevy a rizika:

- mravnostní kriminalita (pedofilie, kyberšikana ad.)

- majetková kriminalita
- zneužívání platebních a obchodních systémů
- porušování autorských práv
- zneužívání dat
- počítačové podvody
- šíření poplašných zpráv
- šíření materiálů se závadným obsahem
- pomluvy a diskreditace
- projevy extremismu
- softwarové pirátství
- síťové hrozby
- zneužívání telekomunikačních postředků

Z pohledu kraje Vysočina je pak aktuální stav problematiky elektronické bezpečnosti možno popsat následující SWOT analýzou.

Silné stránky
- Rozvoj ICT jako politická priorita kraje
- Vůle zájmových skupin řešit problematiku el. bezpečnosti
- Existence pracovní skupiny kraje pro elektronickou bezpečnost

Slabé stránky
- Nevhodné nebo žádné zabezpečení proti elektronickým hrozbám
- Nedostatečné nebo žádné zálohování dat
- Nedostatečně proškolení uživatelů i správců ICT
- Absence legislativy řešící e-bezpečnost na školách a v podnikatelském sektoru
- Nedostatečná informovanost o možném rozsahu škod jako následku nejrůznějších forem zneužití elektronických systémů

Příležitosti
- Zmapovat subjekty, k nimž budou směrovat opatření a aktivity
- Vznik nového krajského ředitelství PČR
- Sběr a analýza dostupných dat souvisejících s bezpečnostními incidenty v kraji a z toho plynoucí rizika
- Možnost získání finančních prostředků pro realizaci projektu e-bezpečnosti

Ohrožení
- Velká šíře problematiky a hrozba ztráty jasného zaměření priorit kraje
- Nejistá národní strategie
- Nedostatek partnerů v ostatních krajích
- Nedostatek odborníků a školitelů v kraji

5. Stanovení priorit kraje v oblasti el. bezpečnosti

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

- Osvěta, prevence a předcházení rizikům…
- Zřízení portálu e-bezpečnosti na webových stránkách kraje Vysočina

- Definice a propagace minimálního standardu pro efektivní ochranu
- Zvyšování povědomí cílových skupin o rizicích, nákladech a nebezpečí vyplývající z e-kriminality
- Vytvoření série vzdělávacích kurzů problematiky elektronické bezpečnosti pro vybrané cílové skupiny a vytvoření sítě školitelů
- Začlenění informací o rizicích e-kriminality do vstupních školení zaměstnanců a vnitřních předpisů organizací
- Pravidelná publikace článků s tematikou e-bezpečnosti pro jednotlivé cílové skupiny v krajských médiích a na portálu e-bezpečnosti
- Získání finančních prostředků na zajištění základních kroků strategie a případný rozvoj problematiky e-bezpečnosti v regionu

6. Akční plán 2010

- Vytvoření systému vzdělávání – kurzy, síť školitelů
- Vznik akreditovaného kurzu el. bezpečnosti pod hlavičkou Vysočina Education
- Zřízení krajského portálu el. bezpečnosti
  - Informační a propagační materiály
  - aktualizované podklady pro školitele
  - životní situace a doporučené postupy (včetně odkazů na dodavatele – web HK)
  - kontaktní systém (formuláře)
  - kontakty pro jednotlivé skupiny
- Průběžná medializace problematiky a aktivit pracovní skupiny

7. Přehled legislativních předpisů

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

- zákon č. 40/1964 Sb., občanský zákoník a jeho prováděcí předpis nařízení vlády č. 258/1985 Sb.,
- 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