evropský sociální fond v ČR EVROPSKÁ UNIE
OPERAČNÍ PROGRAM LIDSKÉ ZDROJE A ZAMĚSTNANOST
Kraj Vysočina
PODPORUJEME VAŠI BUDOUCNOST
www.esfcr.cz

Strategie bezpečnosti ICT kraje Vysočina

číslo dokumentu	**CG_KONS_KAI-102948AR**
datum	30.12.2010
zákazník	Krajský úřad kraje Vysočina

zpracoval

Ing. Karim Ifrah
karim.ifrah@comguard.cz
+420 544 509 062

COMGUARD a.s.
Vídeňská 119b
CZ 602 00 Brno
tel. +420 544 509 059
fax +420 544 509 079
www.comguard.cz

Obsah:

Přílohy:

Příloha č. 1: Metodika analýzy rizik kraje Vysočina
Příloha č. 2: Analýzy rizik kraje Vysočina
Příloha č. 3: SWOT analýza kraje Vysočina

Seznam použitých zkratek

DC – Datové centrum
ICT – informačních a komunikačních technologií
ISDS – informační systém datových stránek
ISVS – informační systém veřejné správy
KrÚ – Krajský úřad
Ntb – Notebook
OI – Odbor informatiky
OKPPCS – Odbor kultury, památkové péče a cestovního ruchu
ORP – Obce s rozšířenou působností
OS – Operační systém
OSK (ODSH) – oddělení správy komunikací (Odbor dopravy a silničního hospodářství)
OSV – Odbor sociálních věcí
OŠMS – Odbor školství, mládeže a sportu
OZ – Odbor zdravotnictví
PO – Příspěvkové organizace
ROP – regionální operační program
TCK – technologické centrum kraje
TCORP - technologická centra obcí s rozšířenou působností
VS – Veřejná správa
VZ – Veřejná zakázka
ZPO – zásadní předmět ochrany
SAN – storage area network
EP – Evropský parlament
ES – Evropská společenství
MVČR – Ministerstvo vnitra ČR
MZČR – Ministerstvo zdravotnictví ČR
AKČR – Asociace krajů České republiky

1. Anotace

Tento dokument je závěrečnou zprávou zpracované analýzy dle zadání pro zjištění aktuálního stavu Tento dokument navazuje na úvodní analýzy prostředí Krajského úřadu a jeho PO ve vybraném vzorku. Cílem tohoto dokumentu je stanovit cílový stav v krátkodobém horizontu a jasně definovat postup, jakým lze tohoto cíle dosáhnout.

Předchozí dokument se zabýval popisem vlastností prostředí a výstupem je tedy charakteristika bodu „0"(horizontální prostředí). V tomto dokumentu navrhujeme změny v čase s cílem dosáhnout širšího pokrytí řešením bezpečnosti prostředí ICT a zavedením kontinuálního procesu řízení bezpečnosti ICT (vertikální prostředí)

Veškerá uvedená zjištění a návrhová část má oporu ve skutečnostech, které jsou detailně uvedeny v přílohách předchozího uvedeného i tohoto dokumentu – analýzy prostředí, analýza rizik, SWOT.

1.1. Definice cíle

Z hlediska definice cíle, **primární cíl** označíme jako **budování bezpečného prostředí** v kraji Vysočina a jeho časová osa není ohraničená – jedná se o kontinuální proces, který je v čase pouze ovlivňován kvalitativně a to v závislosti na vývoji technologií a z toho vyplývající úrovně znalostí. Bezpečné prostředí je vyjádření úrovně bezpečnosti ve smyslu dosažení standardu ISO. Úroveň standardu je charakterizována jako:

- definované a popsané prostředí
- definované a popsané procesy
- definované a popsané kompetence (pravomoc, odpovědnost)
- soulad cílů bezpečnosti ICT s cíli organizace
- kompetentní personál (školený)

Za účelem dosažení primárního cíle stanovíme **sekundární cíle** se shodnou prioritou. Tyto cíle budou pevně ukotveny v čase včetně vyčíslení ekonomické náročnosti. Jsou to konkrétní krátkodobé části, které lze souhrnně označit jako Projekt budování bezpečnosti ICT v kraji Vysočina. Časový rozměr je krátkodobý – 4 roky. V tomto čase budou prováděny zásadní změny v oblasti ICT a v souvisejících oblastech za účelem dosažení primárního cíle. Tyto se budou týkat zejména sjednocení prostředí v jednotlivých oblastech PO a úřadu, vznik subjektu garantujícího bezpečnost informací jako samostatnou disciplínu a dopracování kompletní dokumentace.

1.2. Definice cílových skupin

S předchozího dokumentu vyplývá možné rozdělení ze dvou pohledů. Je z pohledu předmětu činnosti PO anebo z pohledu bezpečnostních charakteristik. Pro účely bezpečnostní strategie je rozhodující pohled na bezpečnostní charakteristiky:

- definice provozu z hlediska rizikovosti
- definice skupin uživatelů
- úroveň významu zpracovávaných informací
- úroveň společenského významu možných ohrožení

Na základě těchto informací navrhujeme pro účely tohoto dokumentu a dalších činností vzhledem k bezpečnosti ICT rozdělit PO do následujících skupin včetně stupně ohrožení ve smyslu řešení bezpečnosti ICT:

Skupina	PO	Stupeň	Pozn.
Kraj - úřad	bez PO	Vysoký	Metodicky vede všechny PO
PO 1 - zdravotnictví	PO v gesci OZ a OSV	Vysoký	Vysoce citlivé informace, kritické aplikace, kritický provoz
PO 2 - školství	Střední školy, školská zařízení a zařízení Soc.věcí	Střední	Citlivé informace, anonymizovaná významná skupina uživatelů
PO 3 - kultura	Muzea, galerie, kulturní zařízení	Nízký	Významný předmět činnosti, konkrétní skupina uživatelů
PO 4 – správa silnic	Správa silnic	Střední	Kritické aplikace, kritický provoz, vliv na provoz na národní úrovni
ORP	Všechny ORP v kraji Vysočina	Vysoký	Společná infrastruktura a provoz TCK a TCORP, sdílení dokumentů a informací

Veškeré informace, ze kterých bylo čerpáno, pro účely tohoto rozdělení jsou uvedeny v dokumentu Komplexní analýza prostředí informačních a komunikačních technologií v kraji Vysočina a jeho příspěvkových organizací včetně příloh.

2. Manažerské shrnutí

Krajský úřad kraje Vysočina patří k subjektům veřejné správy v ČR, které jsou na poměrně vysoké úrovni informatizace. Toto pochopitelně souvisí i s vysokou úrovní vnitřní organizace a managementu. Po provedení všech analytických činností (analýza prostředí, analýza rizik a SWOT analýza) dospíváme k závěru, že to co činí KrÚ tak úspěšným, je zároveň jeho nevětší slabina – jsou to LIDÉ. Na řídících a výkonných pozicích jsou etablování schopní a kompetentní lidé s dostatečnou mírou znalostí, vzdělání a inteligencí, což je zároveň velká hrozba a to v případě fluktuace nebo selhání. Právě lidé jsou nositeli těch nejdůležitějších resp. nejcennějších informací. Pokud tito lidé v procesu naráz chybí, vytvoří informační vakuum a trvá dlouhou dobu, než je tato chyba v organizaci napravena. Tato doba je charakterizována zvýšením časové náročnosti procesů, nekompletními informacemi, zvýšenou náročností na komunikaci a ve svém důsledku vyšší finanční náročnosti. V případě osobního selhání jsou škody dalekosáhlejší a únik informací může mít až fatální následky. Vůbec nejhorší varianta je nastavené průběžné kompromitace systému, tzn. osoba uvnitř organizace kontinuálně zneužívá informace pro svůj prospěch.
Pokud zvážíme vnější faktory ohrožení, pak jsou to opět LIDÉ. KrÚ disponuje prostřednictvím PO velkým množstvím mimořádně citlivých dat, které se mohou stát lákadlem pro jednotlivce či skupiny a to za rozličným účelem (medializace, kriminální činnost, kompromitace atd.).
Je třeba uvést, že data, resp. informace jsou jednak předmětem „businessu" KrÚ ale i jeho nejcennějším aktivem a proto je třeba je nejen mít v aktuální, dostupné a přehledné podobě ale je nutno je i chránit.
Tento dokument se zaměřuje na problematiku bezpečnosti ve vztahu LIDÉ-INFORMACE. KrÚ vytváří prostor pro tento vztah, je vlastníkem informací, které mají lidé resp. zaměstnanci spravovat. KrÚ tedy MUSÍ vytvořit takové prostředí, které bude bezpečné. Toto lze učinit pouze jedinou cestou a to je SYSTÉM ŘÍZENÍ BEZPEČNOSTI. Analýza rizik jasně poukazuje na riziko vnitřního ohrožení dat v kritických aplikacích úřadu. Je to zjevně dáno vzájemným nepoměrem poměrně sofistikované technické ochrany proti neoprávněné manipulaci s daty a nízké úrovně procesního zabezpečení.
V aktuálním prostředí KrÚ je pro zahájení implementace systému řízení bezpečnosti informací velmi příznivé prostředí. Všechny nutné parametry jsou splněny a dále uvedená opatření směřují pouze ke sjednocení řídících procesů bezpečnosti informací a jejich konkretizaci, dosažení standardizovaného prostředí a následná popularizace formou školení a marketingu.
Za nejdůležitější považujeme vznik subjektu ve vnitřní struktuře KrÚ, který bude zajišťovat provoz a kontrolu bezpečnostní politiky KrÚ. Tento subjekt bude představovat výkonnou řídící a kontrolní složku pro oblast bezpečnosti informací. Jeho rolí bude aktualizovat interní legislativu, dohlížet na její dodržování a implementaci a následně kontrolovat a informovat vedení KrÚ o průběžné situaci. Je velmi rizikové ponechat vládu nad bezpečností informací v rukou OI, který spravuje ICT. Praxe ukazuje, že pohled správce ICT na bezpečnost je jiný než vyžaduje skutečnost. Poměrně silným argumentem je fakt, že žádný subjekt není schopen sám sebe účinně auditovat. Pokud opět nahlédneme do analýzy rizik, musíme konstatovat, že vzhledem k výsledkům, si tohoto faktu (možně ne přímo) je si vedení a klíčové osoby v OI vědomo tohoto stavu.
Poměrně závažnou změnu představuje vznik subjektu pro správu sítě ROWANet včetně vzniku centrálního technické podpory, nicméně současnou situaci považujeme za dlouhodobě neudržitelnou. Zde doporučujeme důkladně zvážit způsob změny a jakým způsobem bude řešen majetkoprávní vztah a zda-li řešit tuto záležitost dodavatelský. Jedná se o významné politické rozhodnutí, tudíž bude nutno důkladně analyzovat tuto změnu včetně všech dopadů. Budoucí subjekt by měl spravovat infrastrukturu a poskytovat služby všem připojeným subjektům. Cílem bude zvýšit počet klientů z oblasti VS, kteří by této sítě využívali a zvýšit kvalitu poskytovaných služeb a to včetně provozu centrální technické podpory.
Zřízení jednotky centrálního nákupu nepovažujeme za složité, jde o nastavení vhodných procesů a efektivní orientace na trhu v různých oblastech, aby této služby mohly využívat i PO. Cílem je efektivní nakládání s finančními prostředky a zvýšení transparentnosti při poptávkových či výběrových řízeních.
Realizace navržených opatření nepřekročí 10mil. Kč v roce 2011. tato částka však zahrnuje i nepřímé vnitřní náklady. Přímé náklady – investiční, budou z celkové částky činit asi polovinu. Uvedený finanční objem považujeme s hlediska zkušeností za odpovídající vzhledem k velikosti KrÚ a počtu PO.

V cílovém stavu bude sjednocen dohled nad informacemi, procesy a financemi, tudíž vyšší standard řízení KrÚ. Důsledky z tohoto plynoucí je vyšší konkurenceschopnost, efektivní řízení investic, snižování rizik, zvýšení systémového a systematického zpracování informací a zvýšení image KrÚ.

3. Soulad s nadnárodní, národní, regionální, místní legislativou a příslušnými strategickými dokumenty na všech zmíněných úrovních

Porovnání ve smyslu nadpisu této kapitoly bylo provedeno na úrovni:

- legislativa
- strategie
- projekty

Dostupná a předložená dokumentace byla porovnána v hierarchii:

- Evropská unie
- Obecně platné standardy
- Česká republika
- kraj Vysočina

3.1. Dostupná dokumentace

Prostředí Evropské unie

Legislativa Evropské unie

- Směrnice 1997/66/ES, o ochraně dat v telekomunikacích.
- Směrnice 1995/46/ES, o ochraně osobních dat.
- Směrnice 2002/58/ES, o soukromí v elektronické komunikaci.
- Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy.
- Směrnice 2002/58/ES, o zpracování osobních údajů a ochraně soukromí.
- Nařízení 2001/45/ES, o ochraně fyzických osob při zpracování osobních údajů orgány a institucemi.
- Směrnice rady 1991/250/EHS, o právní ochraně počítačových programů.
- Směrnice rady 2001/264/EC, o ochraně utajovaných informacích
- Nařízení EP a Rady (ES) č. 1007/2008 ze dne 24. září 2008
- nařízení (ES) č. 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací

Strategické dokumenty Evropské unie

- Accelerating the Development of the eHealth Market in Europe (2007)
- CIP ICT-PSP i2010 - Program pro podporu informačních a komunikačních technologií / Evropská strategie pro růst a zaměstnanost

Projekty Evropské unie

- INTEGRANT/mobility
- ERA NET PLUS
- CROSSROAD (FP 7 ICT 2009 Call 4)
- CENTRAL EUROPE
- LEONARDO

Prostředí České republiky

Legislativa České republiky

- 101/2000Sb., o ochraně osobních údajů
- 106/1999Sb., o svobodném přístupu k informacím
- 190/2009 Sb., o archivnictví a spisové službě (změna pův.499/2004Sb.)
- 365/2000Sb., o informačních systémech veřejné správy
- 127/2005Sb., o elektronických komunikacích
- 227/2000Sb., o elektronickém podpisu
- 480/2004Sb., o některých službách informační společnosti
- 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů
- usnesení vlády c. 624 z 20.6.2001, o pravidlech, zásadách a způsobu zabezpečování kontroly užívání počítačových programů
- ústavní zákon 110/1998Sb., o bezpečnosti ČR
- 148/1998Sb., o ochraně utajovaných skutečností
- vyhláška NBÚ 56/1999Sb., o zajištění bezpečnosti informačních systému nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu

Strategické dokumenty České republiky

- Strategie realizace Smart Administration v období 2007–2015 (budování eGovermentu) – (MVČR)
- eGON (Moderní, přátelský a efektivní úřad – MVČR)
- Cíle projektů eHealth v České republice (MZČR)
- Strategie rozvoje informačních a komunikačních technologií (ICT) regionů ČR v letech 2007-13 (2006)
- Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření (MVČR)
- Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení (MVČR)

Strategické projekty České republiky

- budování Technologických center krajů (dále TCK) a obcí s rozšířenou působností (dále TC ORP) v rámci IOP (integrovaný operační program)
- Vzdělávání úředníků a zaměstnanců veřejné správy, metodiků a školitelů a politiků v oblasti zavádění eGovernmentu do veřejné správy v rámci OPLZZ (operační program lidské zdroje a zaměstnanost)

Prostředí kraje Vysočina

Legislativa KrÚ Vysočina

- Informační strategie Krajského úřadu Vysočina
- Informační koncepce Krajského úřadu Vysočina
- Bezpečnostní politika Krajského úřadu Vysočina
- Provozně bezpečnostní dokumentace – bezpečnostní příručka
- Provozní bezpečnostní dokumentace - činnost bezpečnostního správce
- Provozní bezpečnostní dokumentace - bezpečnostní směrnice pro uživatele
- Směrnice k užívání a kontrole užívání informačních a komunikačních technologií kraje Vysočina
- Usnesení RKrÚ
- Organizační řád

Strategické dokumenty KrÚ Vysočina

- Informační strategie KrÚ Vysočina
- Bezpečnostní politika KrÚ Vysočina
- Strategie rozvoje eGovernmentu v kraji Vysočina
- Strategie rozvoje informační společnosti v kraji Vysočina 2009-2013
- Politika rozvoje NGA sítí na území NUTS II. Jihovýchod
- Memorandum o spolupráci (MVČR – AKČR)

Strategicky významné projekty KrÚ Vysočina

- TCK Vysočina
- eHealth
- eCrime
- ROWANet
- Datový sklad KrÚ Vysočina
- Digitální mapa VS
- Digitalizace a ukládání
- Vnitřní integrace úřadu
- Elektronická spisová služba

3.2. Porovnání předložené a dostupné dokumentace

Všechny porovnávané dokumenty vykazují zásadní shodu cílů, postupů a indikátorů. Shoda je dána hierarchií ve vypracování s přímou úměrou k detailu a regionu. Znamená to, že dokumentace i legislativa na úrovni EU je natolik obecná aby poskytla prostor pro regionální specifika. Dokumentace a legislativa na úrovni ČR již uvádí detail charakteristický pro ČR a to zejména legislativa, která je svázána s právním řádem a ústavou ČR. Regionální prostředí kraje Vysočina pouze detailizuje „nadřazené" právní akty a dokumenty pro své prostředí. Detailizace spočívá jednak v úpravě legislativních aktů – tam kde to je legislativou umožněno, na prostředí kraje Vysočina a následně specifikací strategických projektů dle regionálního prostředí kraje.

Pro účely tohoto dokumentu má zásadní význam téma bezpečnosti ICT, kde je nutno konstatovat, že v **oblasti legislativní** je řešena v úrovních:

Úroveň	**Legislativní řešení**	**Hodnocení**
EU	Vyhovující	Existují dostačující doporučení vyplývajících z mezinárodních standardů.
ČR	Nedostačující	Kybernetická bezpečnost není dostatečně ošetřena právním řádem.
KrÚ Vysočina	Formální	Legislativní akty KrÚ obsahují formulace a ustanovení, které částečně řeší bezpečnost informací.

Porovnání strategických dokumentů na uvažovaných úrovních, vykazuje velmi vysokou úroveň shody a v podstatě jsou hierarchicky závislé. Tato závislost je dána částečně provázaností s dotačními zdroji EU a následně ČR, kde čerpání těchto zdrojů je dáno podmínkami uvedenými ve strategických dokumentech. Pokud by tyto podmínky (oblasti, cíle a indikátory) nebyly naplněny, nebylo by možno čerpat tyto finanční zdroje.

Logicky tedy vyplývá z předchozího odstavce, že projekty realizované či plánované k realizaci jsou v plné shodě s projekty na nadřazených úrovních. Toto je dáno i faktem, že vyplývají ze strategických dokumentů KrÚ, které jsou v plné shodě s dokumenty na národní a nadnárodní úrovni.

Porovnání dokumentace KrÚ oproti regionálním, národním a nadnárodním úrovním:

Strategie bezpečnosti ICT kraje Vysočina

Region ⇨ Dokumentace ⇩	**EU**	**ČR**	**Region**
Legislativa	Shoda	Shoda	Doplňuje
Strategie	Shoda	Doplňuje	Doplňuje
Projekty	Doplňuje	Doplňuje	Doplňuje

3.3. Závěr

Průnikem výsledku porovnání této kapitoly s kapitolou č.4 „Analýza právního prostředí bezpečnosti v oblasti ICT" v dokumentu Komplexní analýza prostředí informačních a komunikačních technologií v kraji Vysočina a jeho příspěvkových organizací je konstatování skutečnosti, že právní prostředí v KrÚ je :

- aktuální
- v souladu s legislativou EU a ČR
- v oblastech vztažených k ICT vhodně doplňuje národní legislativu
- odpovídá doporučovaným standardům

Strategické dokumenty a projekty na národní a nadnárodní úrovni jsou v maximální míře promítnuty do strategického řízení a projektů na úrovni KrÚ. Pro účel zvýraznění nalezených skutečností uvádíme zvlášť oblast Strategie, kde:

- zbytečně vysoká míra formalizace tvrzení v dokumentech
- obecné deklarace bez konkrétních údajů - mimo dokumentů zpracovaných v posledních letech (2009/10)
- absence nastavení kontrolních procesů
- nevyvážené propagování všech oblastí ICT

Významná oblast, kde je KrÚ hodnoceno nadprůměrně, jsou projekty. Konkrétně projekty s týkající se ICT jsou v porovnání s národní a nadnárodní úrovní charakterizovány jako:

- vysoká míra kvality projektové dokumentace
- vysoká míra efektivnosti realizace
- detailní provázanost na záměry EU a ČR
- orientace v oblasti financování ze zdrojů EU

Doporučujeme dopracovat interní dokumentaci z oblasti strategických dokumentů a snížit úroveň formálních deklarací, naopak vytvořit konkrétní záměry s možností praktického uvedení do provozní skutečnosti.

Pozn.: Kapitola je zpracována s maximálním ohledem na bezpečnost ICT.

4. Souhrn analýzy stavu úrovně bezpečnosti ICT v kraji Vysočina a v organizacích zřizovaných krajem

Stav úrovně bezpečnosti lze charakterizovat v porovnání s ostatními krajskými úřady jako úroveň „NADSTANDARDNÍ".

Pokud reálný stav porovnáme s obecnou úrovní bezpečnosti v oblasti VS, je tento stav „NADSTANDARDNÍ" a výrazným způsobem odlišný od většiny (>60% - kvalifikovaný odhad) subjektů VS.

S pozice obecného hodnocení a porovnání se zásadami pro budování ISMS vycházejících z ISO 27001 a 27002 je stav charakterizován jako „NECERTIFIKOVATELNÝ".

Zásadními nedostatky jsou :

- odlišná úroveň základního prostředí na KrÚ a PO (lze vzít v úvahu i ORP) s hlediska úrovně ICT
- absence bezpečnostní dokumentace v PO (také ORP)
- formální úroveň stavu bezpečnosti na KrÚ
- absence kontrolních mechanismů z hlediska bezpečnosti ICT
- problematiku bezpečnosti řeší útvar OI

Pozitivní zjištění:

- vývoj aktivit vedoucí k srovnání úrovně ICT alespoň ve skupinách PO (školství, zdravotnictví …)
- aktuální projekty berou v úvahu téma rozvoje bezpečnosti ICT v KrÚ i PO (a ORP)
- technická úroveň zabezpečení KrÚ je na dobré úrovni
- PO se snaží o technické zabezpečení alespoň na finančně dostupné úrovni
- nutnost řešení bezpečnosti ICT si uvědomuje KrÚ i PO (včetně ORP)

Z uvedených zjištění vyplývá, že přímé ohrožení z okolního prostředí není aktuální, interní prostředí LAN KrÚ a LAN PO je zabezpečeno. Komunikační infrastruktura kraje, tedy ROWANet je zabezpečena na dostačující úrovni, nicméně již je místem, kde jsou velmi časté incidenty a trvale se nedaří zabezpečit ji tak, aby nebyla místem vzniku SPAM či místem, odkud je veden a maskován útok na jiný subjekt kyberprostoru. Díky územnímu rozsahu a počtu účastníků na síti ROWANet je zde velmi heterogenní prostředí vzhledem k úrovni technické vyspělosti i zabezpečení. Neexistují striktní pravidla (technická i formální) jako podmínka pro přístup ke službám sítě a neexistuje legislativní dokument pro účastníky, kde by bylo možno zakotvit závazek k „bezpečnému chování v síti".
Díky projektu TCK a TC ORP, který vstupuje v těchto dnech na mnoha místech do poslední předrealizační fáze, bude následovat prudký nárůst nejen subjektů připojených ke krajské infrastruktuře, ale i prudký nárůst provozu na infrastruktuře (objem přenášených dat). Tuto skutečnost je třeba brát v úvahu i z pohledu bezpečnosti ICT. Z technického pohledu je TCK připraveno ve všech ohledech tudíž kapacitně na tuto situaci. Není ovšem řešeno jak má vypadat standard zabezpečení subjektu, který bude ke službám TCK přistupovat (analogie k situaci ROWANet).
Tato situace se zásadním způsobem promítá do výsledků analýzy rizik. Kombinace nadstandardního technického zabezpečení a absence tzv.měkké bezpečnosti vytváří jednoznačný prostor pro útoky zevnitř organizace. Pozitivní je, že díky úrovni zabezpečení jsou tyto útoky identifikovatelné ovšem pak hůře prokazatelné resp. Prokazatelně úmyslné.

Zásadním nedostatkem shledáváme absenci kontrolních mechanismů a kontrolních procesů o více úrovních, které mají za úkol periodicky dohlížet na plnění interních normativů a vyplývajících odpovědností. Tento stav, který lze charakterizovat jako situaci, kde nelze provést audit, je kritický pro případ rozsáhlých incidentů, kde lze způsobit škodu. Hrozbou je, že nelze formou auditu označit pochybení či místo vzniku incidentu a následné odpovědnosti. Tudíž nastává důkazní nouze, kdy nelze prokázat porušení interního pravidla, které není nastaveno (zjednodušeně „není povinnost …").

Konkrétní skupiny dle nastavení v úvodu tohoto dokumentu jsou v oblasti bezpečnosti ICT hodnoceny následovně:

Skupina	**Stav obecně**	**HW zabezpečení**	**Pozn.**
Kraj - úřad	Základní pravidla nastavena a realizována, chybí forma řízené bezpečnosti, koncepce	Vysoký standard	Metodicky by měla vést PO i ORP
PO 1 - zdravotnictví	Nastaven rozvoj bezpečnosti v rámci eHealth, vysoký potenciál ohrožení	V současnosti velké odchylky mezi jednotlivými PO	Vysoce citlivé informace, kritické aplikace, kritický provoz
PO 2 - školství	Velmi obecná pravidla, chybí osvěta mezi žáky, potenciál ohrožení střední ale významný	V současnosti velké odchylky mezi jednotlivými PO	Zásadní roli by měl sehrát projekt eCrime a to formou vzdělávání a dosažení tzv. standardu vybavenosti ICT
PO 3 - kultura	Velmi obecná pravidla, nízké povědomí o bezpečnosti informací	Nízký standard	Zásadní roli by měl sehrát projekt eCrime a to formou vzdělávání a dosažení tzv. standardu vybavenosti ICT
PO 4 – správa silnic	Vysoký standard ICT, obecná pravidla zabezpečení	Vysoký standard	PO zahajuje projekt nasazení standardu na procesní řízení, což je cesta k řízení bezpečnosti
ORP	Výrazné rozdíly, na žádné úrovni nemají dostupný standard či doporučení	Velké odchylky, většinou základ	Zde má KrÚ možnost zaujmout zásadní pozici jako garant bezpečnosti (TC, eCrime)

5. Definice standardu úrovně bezpečnosti při správě a využití ICT

Pro definici standardu zvolíme z hlediska dokumentace, postupů a procesů doporučení ISO 27001 a ISO 27002. Pro definici technického standardu zvolíme návrh na základě nejlepších zkušeností ověřených na implementacích bezpečnostních řešení na úrovni nadnárodní tak národní s přihlédnutím na specifika subjektů veřejné správy v ČR na regionální úrovni. Vycházíme zde z výsledků analýzy rizik, která jasně specifikuje jako největší rizikovou oblast DATA a zdroj ohrožení UŽIVATEL. V následujícím textu budeme proto klást důraz na doporučení, která eliminují zmíněné riziko.

5.1. Standard řízení bezpečnosti ICT

Rozdělení řešení bezpečnosti na oblasti:

a) vnější
b) vnitřní

tyto základní části se obě dále dělí na:

1. technickou
2. procesní

Všechny části jsou nedělitelně provázány a tvoří funkční celek.
Pro implementaci standardu bezpečnosti je třeba vytvořit SYSTÉM ŘÍZENÍ BEZPEČNOSTI ICT. Základem tohoto je aktuální dokumentace, která musí obsahovat:

- Bezpečnostní politika
- Směrnice pro řízení bezpečnosti (lze aplikovat do provozního řádu)
- Technická dokumentace (kompletní a průběžně aktualizována)
- Provozní dokumentace (vedení záznamů o nastaveních, provozu a změnách)

Tato dokumentace musí reflektovat skutečný stav v organizaci a dále se členit dle organizační struktury a specifikovat detaily pro konkrétní úroveň.

Správa technických prostředků bezpečnosti musí být zakotvena v provozní dokumentaci, kde je také stanovena hierarchie zodpovědností a postupy pro případ vzniku incidentu včetně kompetencí konkrétních pracovníků.

Jednotlivé technické prostředky jsou nastaveny tak, aby bylo zřejmé, které bezpečnostní činnosti vykonávají, jaké jsou výstupy z těchto činností a jakým způsobem jsou zpracovány a využity.

Důležitým aspektem Systému řízení bezpečnosti je možnost průběžného AUDITU. Zásadním pravidlem je oddělení subjektu organizace, který prování správu a provoz technické infrastruktury a prostředků ICT od subjektu vykonávajícího roli řízení bezpečnosti informací. Vždy je nutno řídit se pravidlem, že „provozní organizační jednotka nemůže sebe sama kontrolovat". Tento stav je vysoce rizikový.

5.2. Standard úrovně technického zabezpečení

Současné nastavení technické úrovně KrÚ je na dostatečně vysoké úrovni, proto tento návrh je spíše formalizací již provozované skutečnosti a neobsahuje technické parametry. Analýza rizik toto potvrzuje a rizika spojená s technickou úrovní jsou na akceptovatelné úrovni.
Naopak pro skupinu PO návrh obsahuje konkrétní technické parametry na minimální úrovni, zde vycházíme z výsledků analýzy prostředí PO. Filosofie návrhu vychází ze zásad standardizace a centralizace systému řízení bezpečnosti.

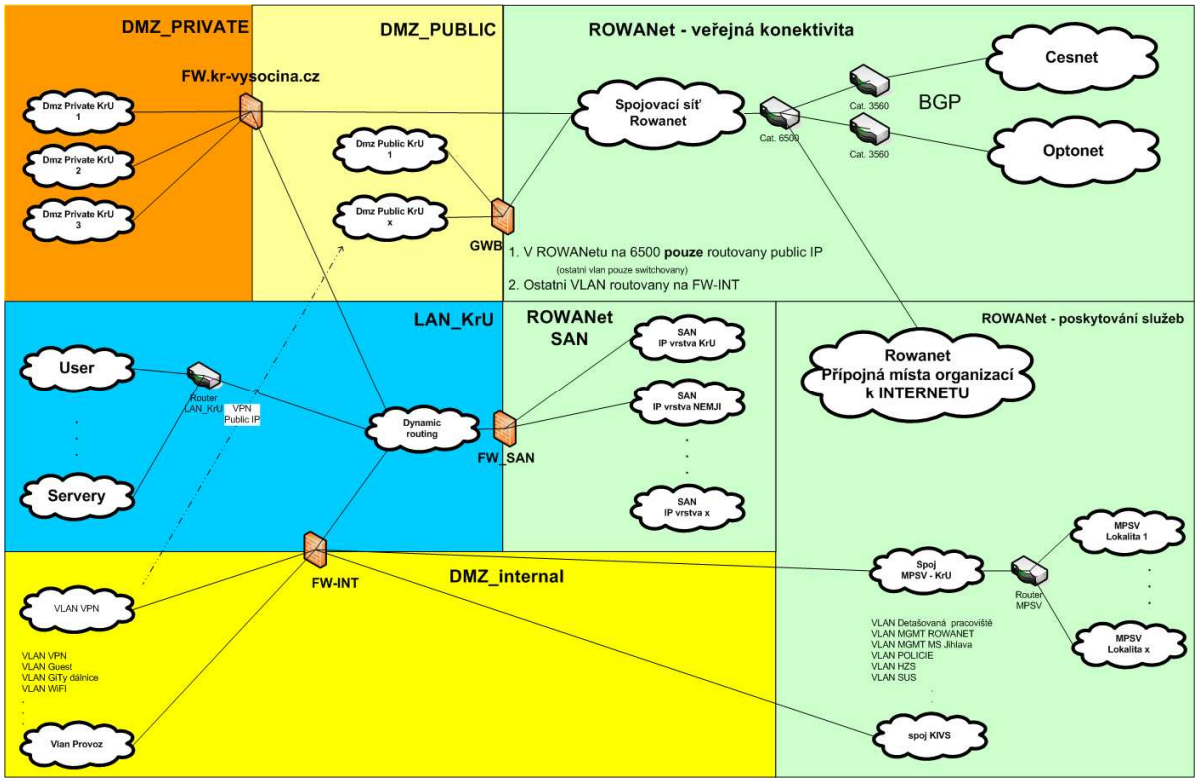
5.2.1. Úroveň technického zabezpečení KrÚ

Pro účely této kapitoly vzhledem k úrovni zabezpečení všech částí infrastruktury KrÚ považujeme za důležité zdůraznit pouze zásady pro budování technického zabezpečení sítí:

Obecná pravidla:

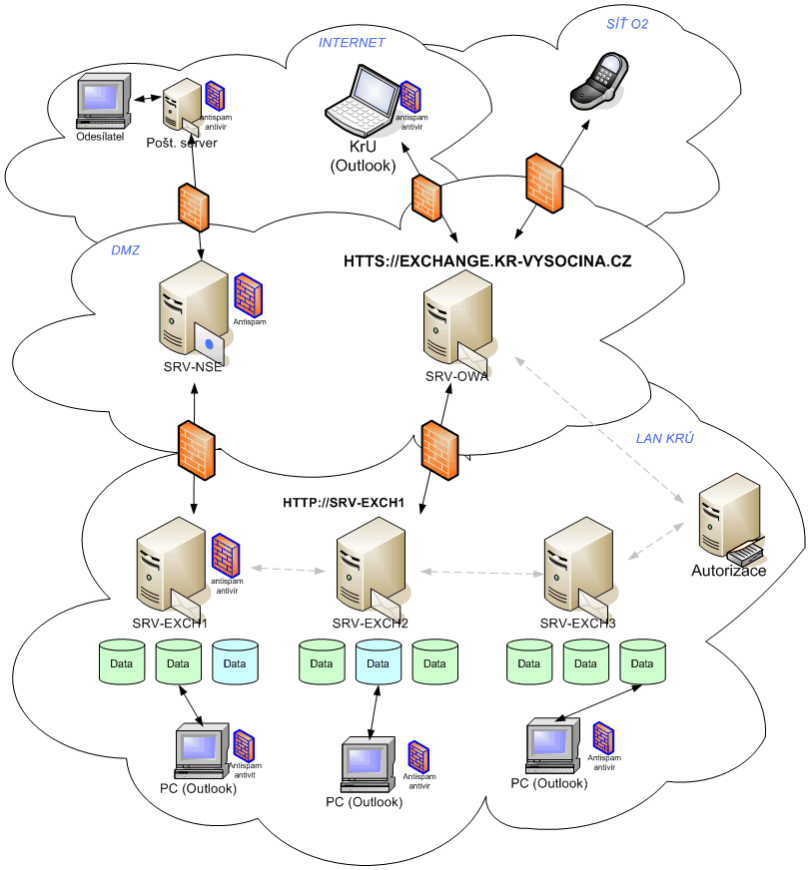
- Centrální Firewall (dále FW) v clusteru, včetně DMZ
- FW včetně DMZ na dalších segmentech Extranetu
- Využití Proxy
- Vhodná segmentace sítě (VLAN)
- Monitoring provozu Extranet prostřednictvím IDS/IPS
- Centrální správa bezpečnostních prvků
- Monitoring aktivních prvků (včetně sběru a kontroly logů)
- Monitoring obecného provozu
- Ochrana aplikací v DMZ
- Zabezpečení antiX
- Filtrace šifrovaného provozu
- Promyšlená virtualizace (systém práv)
- Zajištění bezpečného vzdáleného přístupu (VPN)

Logické schéma **infrastruktury KrÚ** :



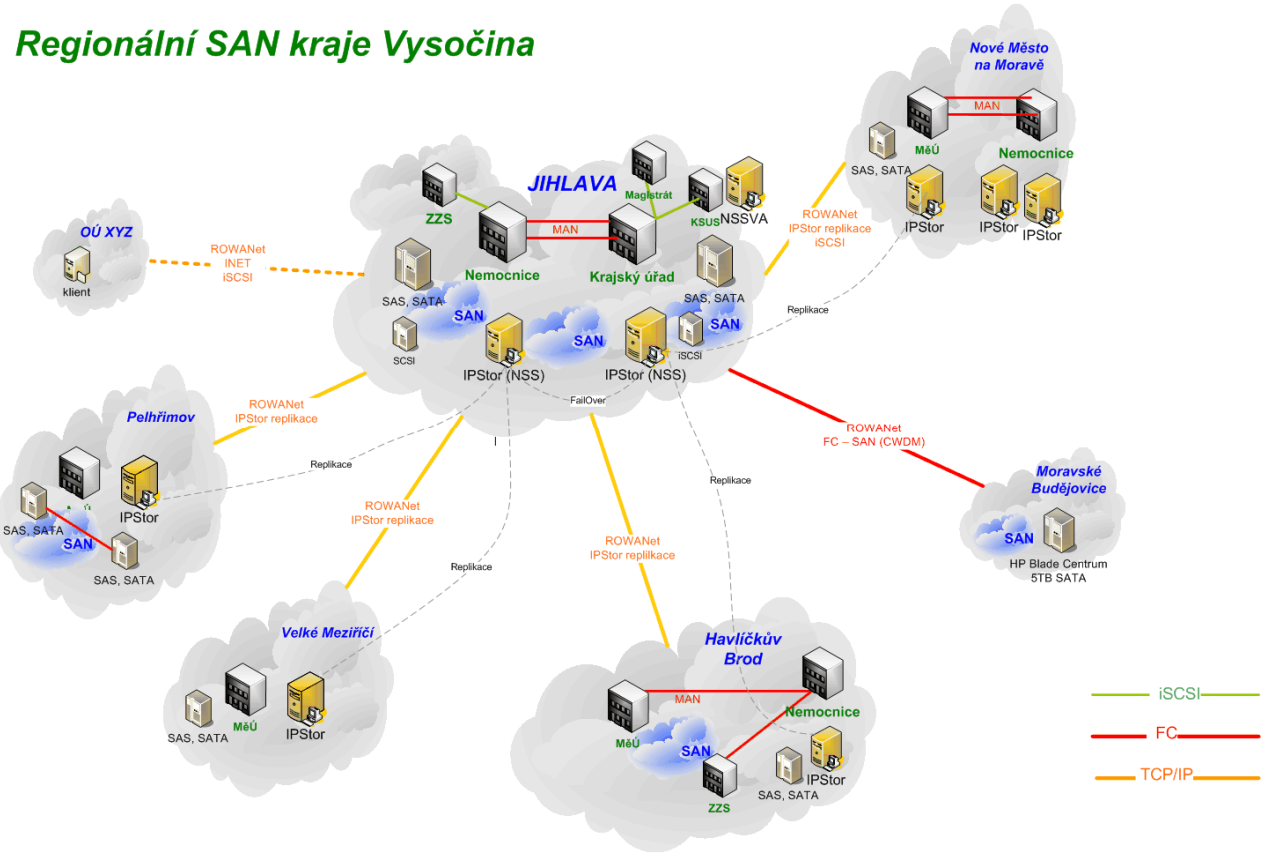
Standard technického zabezpečení nastavený na infrastruktuře uvedené ve schématu lze prohlásit za plně vyhovující.
Doporučit lze implementaci nástroje Risk managementu pro řešení správy rizik a řízení zranitelností jednotlivých prvků sítě.
Další vhodnou komponentou je ochrana webového provozu – aplikační FW.

Logické schéma zabezpečení ochrany **systému el. komunikace** :



Zabezpečení systému el. komunikace je plně vyhovující současnému standardu úrovně technického zabezpečení.

Schéma SAN KrÚ:



Pro účely zajištění ochrany SAN doporučujeme nasadit produkty pro monitoring provozu (chování uživatelů) a ochranu dokumentů.

Vysoký standard současné ochrany technickými prostředky neumožňuje taxativní doporučení funkcionalit technických prostředků pro zajištění bezpečnosti. Personál spravující tuto oblast je dostatečně kompetentní a je schopen analyzovat potřeby vzhledem ke všem parametrům provozovaných ICT prostředků a následně nastavit požadavky na technické parametry konkrétních zařízení.

5.2.2. Úroveň technického zabezpečení PO a ORP

Pro dosažení stavu řízení bezpečnosti je třeba sjednotit alespoň parametricky (technologicky není nutno) úroveň zabezpečení subjektů. Tato úroveň bude následně zakotvena v dokumentaci a směrnicích pro provoz na infrastruktuře KrÚ resp. na síti ROWANet a TCK.

Standard zabezpečení navrhujeme rozdělit dle výše identifikovaných skupin:

Skupina	Perimetr	Interní bezpečnost	Specificky
PO 1 - zdravotnictví	- FW „hi-tech“ - ochrana eMail - DMZ - AntiX - Aplikační filtr - cluster řešení	- IPS/IDS sondy - Risk management - DLP (ochrana dat) - Personal FW	Imaging PC a Ntb včetně kontroly, Management aktivních prvků, IDM, striktní oddělení Public systémů – např.Wifi, důsledná ochrana vzdálených přístupů.
PO 2 - školství	- FW standard	- segmentace sítě	Důsledný imaging stanic a

	- DMZ - AntiX	- ochrana stanic	jejich periodické „čištění" v krátkých intervalech.
PO 3 – kultura	- FW standard - AntiX	- segmentace sítě - ochrana stanic	Oddělení Public systémů, filtrace web provozu uživatelů a důsledná autentikace
PO 4 – správa silnic	- FW druhé generace - ochrana eMail - DMZ - AntiX - Aplikační filtr - cluster řešení	- IPS/IDS sondy - Risk management - DLP (ochrana dat) - ochrana stanic	PO zahajuje projekt nasazení standardu na procesní řízení, což je cesta k řízení bezpečnosti
ORP	- FW druhé generace - ochrana eMail - DMZ - AntiX - Aplikační filtr	- IPS/IDS sondy - DLP (ochrana dat) - ochrana stanic	Segmentovaná síť, implementované IDM, chráněné externí přístupy VPN

Definice funkcionalit zařízení:

FW standard:

- Předinstalované řešení typu appliance (hw + software) certifikací dle ISO 15408 Common Criteria EAL na úroveň 4+ včetně certifikace pro Application-level Firewall Protection Profile
- schopnost práce v Fail Over Clusteru v automatických režimech Active/Active s rozkladem zátěže a podpora i režimu Active/Standby
- Reporter nástroj pro Security Events Management (SEM) událostí a jejich konsolidace a korelace ze všech dodaných firewallů (Firewall reporter)
- Profiler nástroj pro zjištění efektivity nastavení pravidel, korelující srovnání provozu v nastavených časových zónách a zobrazující vliv nastaveného pravidla na tento provoz s možností snadného zobrazení kdo využívá provoz jakých aplikací a rychlé zjištění zda problém byl způsoben firewallem nebo navigaci ke zdroji problému
- Integrovaná Antivirová kontrola nastavitelná per proxy (nesmí být open source) pro neomezený počet uživatelů a protokoly http, https, smtp a ftp
- Požadována plnohodnotná IPS kontrola na firewallu nastavitelná individuálně per pravidlo s možnosti vybrat konkrétní signatury pro typ provozu (webový provoz, emailový, databáze, backup servery aj)
- Filtrování provozu dle URL kategorií na základě denně aktualizovaného kategorizovaného seznamu URL adres zahrnující i kategorie bezpečnostní tj Malware stránky (ochrana proti hrozbám z web provozu), i volnočasové jako on-line hry, chaty, IM, on-line radia a televize apod.
- Integrovaný systém ochran umožňující zakázat (povolit) komunikaci z/na IP adresy dle jednoduchého zadání geografické lokality (například integrovaný seznam zemí)

FW hi-tech:

- Předinstalované řešení typu appliance (hw + software) se zabezpečeným operačním systémem a certifikací dle ISO 15408 Common Criteria EAL na úroveň 4+ včetně certifikace pro Application-level Firewall Protection Profile
- schopnost práce v Fail Over Clusteru v automatických režimech Active/Active s rozkladem zátěže a podpora i režimu Active/Standby
- Implementována proxy kontrola pro http, https, smtp, SSH, Oracle, ICA (Citrix), FTP, SIP, H323, MS SQL s nastavením parametrů kontrol uvnitř protokolu (např. zakázání příkazů post u http protokolu apod)
- Bezpečnost pro SSH - dešifrování a kontrola SSH a následné zašifrování

- Bezpečnost pro HTTPS - dešifrování a kontrola SSL (HTTPS) provozu (dešifrování na firewalu) a schopnost opětovného zašifrování, (nejen pro provoz směřující na severy v LAN, DMZ ale i pro provoz klientů organizace přistupující na externí weby přes https (např na **https://mail.seznam.cz** apod)
- Nastavování politik dle Identit. Schopnost zařízení přebírat Identity z MS Domeny (Active directory) bez požadavku na opětovnou autentizaci. Politiky jsou nastaveny dle skupin uživatelů nebo jmen v AD.
- Optimalizace pravidel v reálném čase - eliminace duplicit, konfliktů a přesahujících pravidel
- kontrola VoIP provozu (SIP a H323 proxy)
- aplikační firewall (kontrola na aplikační úrovni s využitím aplikačních proxy bran, tj spojení je terminováno na firewallu a proxy firewallu vyjedná nové spojení) s možností kontrol na nižších vrstvách OSI modelu (paketová filtrace, stavová inspekce). Kontrola pro příchozí i odchozí internetový provoz s ochranou bezpečnosti provozu od 3. do 7. vrstvy OSI modelu
- Identifikace aplikací a možnost nastavení provozu (whitelisting) dle konkrétních aplikací a uživatelů/skupin (například i v rámci web provozu) na základě jejich signatur s možností granulárního řízení povolených funkcí v rámci aplikace (například možnost vypnout file sharing v rámci IM). Požadováno rozpoznání minimálně 1000 signatur aplikací. Možnost kontroly provozu v rámci aplikací i při jejich šifrování (https)
- Reporter nástroj pro Security Events Management (SEM) událostí a jejich konsolidace a korelace ze všech dodaných firewallů (Firewall reporter)
- Profiler nástroj pro zjištění efektivity nastavení pravidel, korelující srovnání provozu v nastavených časových zónách a zobrazující vliv nastaveného pravidla na tento provoz s možností snadného zobrazení kdo využívá provoz jakých aplikací a rychlé zjištění zda problém byl způsoben firewallem nebo navigaci ke zdroji problému
- Integrovaná Antivirová kontrola nastavitelná per proxy (nesmí být open source) pro neomezený počet uživatelů a protokoly http, https, smtp a ftp
- Plnohodnotná IPS kontrola na firewallu nastavitelná individuálně per pravidlo s možnosti vybrat konkrétní signatury pro typ provozu (webový provoz, emailový, databáze, backup servery aj)
- Firewall umožňuje provozovat zabezpečené SMTP servery (např sendmail přímo on box), které budou plnit funkci interního a externího smtp serveru a budou chráněny zabezpečeným OS firewallu a automaticky patchovány přímo s firewallem
- Firewall umožňuje poskytnout resolvovani doménových jmen na zařízení s vysokou mírou zabezpečení (například split servery), tj provozovat zabezpečené DNS servery (např bind on box), které budou plnit funkci interního a externího DNS serveru a budou chráněny zabezpečeným OS firewallu a automaticky patchovány přímo s firewallem.
- Filtrování provozu dle URL kategorií na základě denně aktualizovaného kategorizovaného seznamu URL adres zahrnující i kategorie bezpečnostní tj Malware stránky (ochrana proti hrozbám z web provozu), i volnočasové jako on-line hry, chaty, IM, on-line radia a televize apod.
- integrovaný systém ochran pomocí globálních reputací minimálně pro smtp a http/https provoz, integrovaný per pravidlo, umožňující omezit nebo zakázat provoz ze systémů se špatnou reputací (botNet nebo zombiePC sítě)
- Integrovaný systém ochran umožňující zakázat (povolit) komunikaci z/na IP adresy dle jednoduchého zadání geografické lokality (například integrovaný seznam zemí)

Ochrana e-Mail:

- Provoz chráněn v obou směrech
- Anti-Spam & Phishing kombinace více různorodých metod s možností podrobného nastavení odhalující nevyžádanou poštu
- Dynamická nastavení kontrol aktualizace antispamových algoritmů v časové periodě 20 min
- Anti-Virus & Spyware filtr, obousměrná ochrana proti škodlivým kódům v poštovním provozu
- IPS & Firewall řešení se sadou nástrojů chránících poštovní servery proti hackingu

- Proaktivní i reaktivní ochrana pošty před viry, trojany, červy aj. Web born malware, DoS útoky, Directory harvests útoky, phishingem…
- Ochrana citlivých dat inteligentní technologie chrání citlivá data proti úmyslnému i neúmyslnému úniku
- Ochrana Web Mail – vestavěné ochrany pro MS OWA, LNWA,…
- Globální inteligence díky napojení na systém globálních reputací TrustedSource se využívá znalosti chování subjektů na Internetu, identifikují se podezřelí a nelegitimní odesílatelé (např. zombie PC, botnety, …), kteří jsou díky tomu blokování bez nutnosti lokálních analýz
- Kontrola emailových adres na základě LDAP dotazů vůči adresářové struktuře (MS AD,…)
- Filtrace obrázkového spamu chrání uživatele před obrázkovým spamem

DMZ:

Servery pro komunikaci s okolním světem (internet, extranet, vzdálený přístup atd.) jsou umístěny v izolované zóně tak, v případě napadení došlo pouze k poškození či vyřazení na těchto serverech. Tzv. živá data jsou umístěna na serverech v LAN jsou do DMZ replikována. Pro řešení s vysokým stupněm ohrožení je vhodné umístit do DMZ i IPS/IDS. V DMZ se odehrává veškerý web provoz.

AntiX :

- ochrana proti nebezpečným kódům formou kontroly webového provozu (HTTP, HTTPS, FTP).
- Globální inteligence - proaktivní detekce s napojením na systém globálních reputací.
- Web & DNS Cache proaktivní kontrola a testy reputace objektů před doručením uživatelům.
- AntiMalware – hloubkový výkon proaktivní antimalware ochrany proti virům, červům, trojským koňím a špiónům.
- AntiVirus - filtrace se skenováním a online kontrolou spustitelných souborů (v reálném čase).
- URL filtrace – výkonné, vícejazyčné filtrování webového obsahu s využitím databáze a hodnocením webů podle skóre.
- Inspekce HTTPS (SSL šifrovaného provozu) - dočasné dešifrování odchozího i příchozího HTTPS provozu, následná kontrola obsahu včetně kontroly certifikátů a opětovné zašifrování, čímž je zachována důvěrnost dat.
- Instant Messaging (IM) Proxy – ochrana pro nejvíce rozšířené IM protokoly (MSN, Yahoo).
- Streaming Proxy – nativní ochrana streamovaných médií s podporou pro RTSP – doručování dat v reálném čase (zvuk, video); MMS s děleným streamováním a cachováním.
- Politika pravidel – engine založený na politice pravidel s vysokou granularitou a objektově orientovaným přístupem.
- Filtrování pro mobilní uživatele za účelem kontroly přístupu na web pro mobilní uživatele.

DLP:

- Identifikace rizik ztráty dat
  - skenuje informace uložené na všech dostupných úložištích
  - identifikuje, kde se citlivá dat nacházejí a kdo je vlastníkem těchto dat
  - vyhledávání a prohlížení všech skenovaných dat je podpořeno intuitivním rozhraním
- Vytváření politik a reportů
  - na základě vyhledaných dat transformuje výsledky to ochranných pravidel
  - politiky chránící intelektuální vlastnictví společnosti v elektronické podobě
- Klasifikace, analýza a eliminace rizik
  - filtruje a kontroluje citlivá data bez multi-vektorové klasifikace
  - indexuje všechen obsah a poté v něm vyhledává důvěrné informace

  - registruje a vytváří signatury k ochraně dokumentů a informací v nich obsažených i tehdy, jsou-li kopírovány či měněny
  - zasílá upozornění v případě, že jsou porušeny pravidla ochrany dat
- Identifikace a ochrana citlivých dat
  - identifikuje důvěrné informace skrze intuitivní vyhledávací systém
  - řídí forenzní analýzy pro korelaci současných a minulých rizikových událostní, detekuje rizikové trendy a identifikuje hrozby
  - okamžitě vytváří pravidla pro prevenci budoucího chování
- Průzkum a indexace veškerého síťového provozu
  - filtruje a kontroluje citlivé informace pro odkrytí skrytých či neznámých rizik
  - indexuje všechny typy provozu a umožňuje vyhledávání pro bližší porozumění citlivým datům včetně toho, kam jsou posílána
  - monitoruje přístup k interním sdíleným souborům
- Tvorba a ladění sofistikovaných pravidel
  - identifikuje velké množství unikátních typů obsahu na jakémkoli portu či aplikaci
  - klasifikuje síťový provoz nezávisle na portu
  - podpora stovek tisíců současných spojení

Ochrana stanic a serverů:

Moderní řešení pro zajištění interní bezpečnosti musí zahrnovat i ULR filtering, šifrování notebooků, Policy auditing a bezpecnost pro Groupware jako je exchange a servery.

10 požadavku na moderní systém ochran pro interní prostředí (desktopy, servery, groupware, auditing) s požadavkem na jednotnou správu:

1. Anti-Virus & Spyware
1. Email server Anti-Virus & Anti-Spam (Exchange/Lotus)
2. Desktop sw IPS & Desktop Firewall
3. Device Control řízení připojitelných zařízení typu USB, wifi, Bluetoth
4. Encryption for PC (šifrování celých disků)
5. Web Filtering (řízení přístpu na web stránky pomocí kategorií zabrání přístupu na stránky s pornografií a malware
6. NAC (zajištění přístupu do sítě pro autorizované počítače splňující definované požadavky)
7. Policy Auditor - Audit stavu počítačů (hesla, patche, přítomnost a aktuálnost bezpečnostních systému apod)
8. AV ochrana pro file servery (Windows a Linux)
9. Jednotná centrální správa s vynucením politik pro všechny komponenty a jednotná reportovací správa zajisťující jednotný přehled o událostech v síti včetně dodaného fw

5.3. Standard úrovně procesního zabezpečení

Zásadními opatřeními pro fungování řízení bezpečnosti jsou:

1. Bezpečnostní politika
2. Organizace bezpečnosti
3. Klasifikace řízení aktiv
4. Personální bezpečnost
5. Fyzická bezpečnost a bezpečnost prostředí
6. Řízení systémů
7. Řízení přístupů
8. Vývoj a údržba systémů
9. Řízení incidentů

10. Řízení kontinuity organizace
11. Soulad s požadavky

Dále v textu bude specifikována do jaké míry je vhodné pro KrÚ implementovat opatření – definovaný standard.

1. Bezpečnostní politika

Základní strategický dokument určující cíle, směr a principy bezpečnosti.

Je založena na:
- strategii organizace
- požadavcích na informační bezpečnost
- bezpečnostní požadavky partnerů, nadřízených orgánů a třetích stran
- zákonech, standardech a dalších obecně závazných předpisech

Obsahuje:
- definici informační bezpečnosti, její cíle a rozsah, její důležitost
- deklaraci o podpoře managementem
- shrnutí požadavku a principu vyplývající z legislativy a standardu
- definici zodpovědností
- kritéria pro hodnocení rizik
- systém pro reportování bezpečnostních incidentu
- odkaz na další dokumenty

2. Organizace bezpečnosti

Pro řízení bezpečnosti je sestaven projektový tým, který ji má na starosti. Bezpečnost musí rocházet celou organizací, takže vlastnící klíčových procesu.

Organizace:
- sponzor projektu (člen top-managementu)
- manažer projektu, koordinátor projektu
- ostatní členové týmu (viz. vlastníci klíčových procesů)
- Možnost zapojení externí poradenské firmy. Zkušenosti s únikem informací.

Vrcholový management musí:
- podporovat zavedení
- spolupracovat na bezpečnostní politice
- zajistit vytvoření bezpečnostních cílu a plánu
- komunikovat inf. bezpečnost v celé organizaci
- zajistit dostatečné zdroje
- rozhodnout o přijatelné úrovni rizika
- kontrolovat management bezpečnosti
- ostatní musí dodržovat bezpečnostní politiku.

3. Klasifikace řízení aktiv

Provedená důsledná inventarizace majetku souvisejícím s provozem ICT a to včetně jednoznačné identifikace. Každé aktivum by mělo mít svoji přiřazenou odpovědnou osobu a místo.

Taktéž je nutno provést inventarizaci dat a informací, klasifikovat je a přiřadit jim zodpovědnou osobu. Výsledkem tohoto procesu je jednotné a jednoznačné označování dokumentů, záznamů či souborů a tím dosažená přehledná struktura dat a informací.

4. Personální bezpečnost

Zde heslovitě uvádíme zásady pro vhodnou strukturu personální politiky :

- bezpečnost jako součást popisu prac. pozice včetně odpovědností (promítnutí do prac.smluv)
- na kritických pozicích prověrky zaměstnanců
- dohody o důvěrnosti
- popisy pracovních míst
- odpovědnost managementu
- školení
- disciplinární řízení (postupy)
- změny a ukončení zaměstnaneckého poměru (postupy)

Pozn. Úroveň prověrky zaměstnanců je dle zvážení a zkušenosti či potřeby KrÚ. Je možno vycházet z běžně užívaného standardu „změkčeného" dle potřeby, nebo postačí např. psychologické testy.

5. Fyzická bezpečnost

Tato kapitola se dotýká primárně provozu datových center a okrajově provozu v administrativních budovách KrÚ. Zde je etalon bezpečnosti popsán v dokumentaci pro budování TCK a TC ORP. Za účelem nastavení standardu je tato úroveň vyhovující. Zásadními tématy k zajištění jsou:

- zajištění monitorování fyzických přístupů
- automatický protipožární systém
- redundance chladícího systému
- redundance napájení
- odolnost proti živelným katastrofám (voda, požár atd.)
- monitoring provozu

6. Řízení systémů

Deklarujeme okruhy, které je potřeba řešit formou „popis – provoz – odpovědnost – kontrola". Není nutno pro účely řízení bezpečnosti jít do absolutního detailu, je třeba na reálné úrovni zachytit stav věcí a stanovit kompetence. Konkrétní návod je popsán v dokumentaci ISO 2700x, kde lze zvolit i požadovanou úroveň detailu.

- provoz
- cyklus : vývoj, testování, nasazení, rutinní provoz
- ochrana před Xware
- správa infrastruktury
- správa stanic
- ukládání, distribuce, transport a zálohování dat
- monitoring

7. Řízení přístupů

Základním požadavkem je nastavení IDM (identity management systém) pro kontrolu nad uživateli a jejich právy. Součástí systému řízení bezpečnosti musí být jednoznačný popis práv a rolí v hierarchii KrÚ, PO a ORP. Tyto popisy budou existovat odděleně, nicméně jejich existence zajišťuje následně

jednoznačnou identifikaci. Přístupová práva jsou členěna v souvislosti s pracovním zařazením a jsou ukotvena v popisu pracovní náplně (pozice).

U zařízení, prostředků a informačních zdrojů jsou jednoznačně definovány uživatelské skupiny a k nim jsou jednoznačně přiřazeny seznamy práv a rolí.

Role a práva uživatelů jsou popsána a přiřazena konkrétním uživatelům.

Pokud je toto zachováno, lze jednoduchým postupem „křížovou metodou" ověřit správnost nastavení a oprávněnost role či práva.

Každý uživatel, zařízení či aplikace v systému musí být jednoznačně identifikovatelná.

Rozdělení práv a rolí musí být sjednocena na úrovni terminologie mezi všemi subjekty kraje (KrÚ, PO, ORP).

Veškeré přístupy mezi sítěmi (vstup do ROWANet) musí být řízeny přes bezpečnostní prvky (FW, filtr) a důsledně logovány. Logy je třeba analyzovat a vyhodnocovat.

Pro přístupy do počítače či sítě musí být nastaveny jasné postupy pro „přihlášení". Týká se to i přístupů VPN.

Pravidelný monitoring provozu, včetně vyhodnocení a stanovení postupů při porušení pravidel.

8. Nákup, vývoj a údržba

V této kapitole se omezíme na označení základních činností, pro které by měla být stanovena pravidla. Procesy by měly být popsány a o provedeném procesu by měl existovat zápis se stanovením závěru a doporučení.

- analýza
- požadavky
- testování
- dokumentace
- změny
- servis (údržba)

Pro servisní činnosti je důležité stanovení tzv.SLA (service level agreement), která představuje úroveň dostupnosti služby, aplikace či zařízení (nebo systému) v závislosti na čase. Stanovení této hodnoty závisí od mnoha vlivů, nicméně pro účely doporučení uvádíme, že hodnota SLA by neměla být nižší než 95.

Pro zajištění uvedených skutečností je doporučujeme všechny tato činnosti sjednotit do jednoho „kanálu". Výhodou je 100% kontrola nad uvedenými činnostmi a ekonomické výhodnost (objemové slevy). Tímto je dosaženo nákupu ověřených technologií s garantovaných zdrojů. Dalším faktorem je minimalizace heterogenních řešení pro ICT kraje.

9. Řízení bezpečnostních incidentů

Předpokladem pro udržení standardu bezpečnosti je zavedení centrální technické podpory pro ROWANet a zajištění řízení incidentů formou „trouble ticketu". Princip fungování je zachycení události – incidentu od okamžiku vzniku až po ukončení – vyřešení. Je třeba stanovit definici druhů incidentů a způsobů jejich řešení, dále je důležité nastavit standardní procesy pro standardní incidenty (výpadek, výměna toneru, nedostupná aplikace …atd.) a nakonec definice kdy je incident ukončen a to včetně vyjádření majitele

aktiva. Je dále třeba navrhnout procesy a komunikaci mezi stávajícím HelpDesk KrÚ s „Centrální technickou podporou, která bude nedílnou součástí Kompetenčního centra (v budoucnosti).

Pro zavedení této instituce je třeba mít katalog služeb s jasnou definicí služeb. Poté je vhodné mít k dispozici rozpad na jednotlivé dodavatele služeb (externí, interní) a definice okruhu uživatelů.

10. Řízení kontinuity organizace

Toto opatření představuje nutnost provázání systému bezpečnosti ICT na opatření k periodickému snižování rizik a na krizové plánování. Znamená to promítnutí aspektů bezpečnosti informací do Systému řízení krizových situací.

11. Soulad s požadavky

Veškerá opatření týkající se systému řízení bezpečnosti ICT musí být v souladu s legislativou a zájmy organizace. Legislativa musí být definována – konkrétní ustanovení, které je třeba promítnout do systému řízení bezpečnosti, dodržovat a kontrolovat.
Kritická místa a procesy musí být jasně definovány a k nim přiřazena patřičná opatření.
Nástroje pro provozní audit systému by měly být odděleny od běžných provozních nástrojů aby neumožnili kompromitovat provozní systém, systém musí být nastaven tak aby byl těmito nástroji auditovatelný. Výstupem z auditu by měla být klasifikace nastavení systému a následná doporučení ke zvýšení kvality opatření.

6. Definice opatření (přínosy cílovým skupinám), návrh harmonogramu

V návaznosti na předchozí doporučení je třeba definovat konkrétní opatření a aplikovat doporučení do prostředí KrÚ, PO a ORP. Dále uvedená doporučení vycházejí nejen z tohoto dokumentu ale hlavně z provedených analýz a závěrů uvedených v dokumentu Komplexní analýza prostředí informačních a komunikačních technologií v kraji Vysočina a jeho příspěvkových organizací. Tato opatření uvádíme bez rozdělení mezi jednotlivé subjekty, neboť iniciátorem a garantem navržených opatření bude KrÚ.

6.1. Legislativní opatření

- Je třeba aktualizovat strategické dokumenty KrÚ tak, aby jejich obsah odrážet reálný stav ICT v organizaci a dosažení reálných cílů. Popsat jejich promítnutí směrem k PO s patřičnou argumentací.
- Bezpečnostní politika KrÚ musí být přepracována tak, aby odrážela skutečný stav ICT, musí obsahovat konkrétní nastavení procesů a odpovědností. Toto lze dosáhnout přepracováním podřízených dokumentů a tam lze aplikovat větší detail. Součástí bude doporučení či vzor pro skupiny PO, tak aby bylo možno zaháji proces jejich integrace do krajského systému řízení bezpečnosti (vyhovující by byla tzv. ratifikovatelná forma). Zakotvení periodické povinnosti vzdělávání.
- Dokončit vydání nové verze provozního řádu, kde by měl být bezpečnosti věnován větší prostor. Provozní řád by měl mít část TCK, LAN a ROWANet rozdělenou na závaznou část pro připojení a užívání služeb a část doporučující pro provoz LAN PO a ORP s vazbou na ROWANet.
- Nastavit kontrolní a auditní mechanismy pro provoz ICT (včetně OI)
- Školení personálu ve všech cílových skupinách

Přínosy:

Pro potřeby standardizace je nutno mít oporu ve strategických dokumentech a interní legislativě. Tyto dokumenty musí projít schvalovacími procesy KrÚ aby se staly závazné pro všechny zúčastněné subjekty. Zahájený proces budování řízeného systému bezpečnosti informací bude kontinuální a kontrolovatelný. V dokumentech bude jasně specifikován záměr společně s cílovým stavem. Zakotvená pravidla a opatření budou vymahatelná a celý systém se tímto stane řiditelným.
Všechny zúčastněné subjekty budou mít dostupnou konkrétní informaci o nastavené úrovni bezpečnosti ICT v kraji. Tento standard se stane automaticky závazným i pro všechny připravované projekty či vstupující subjekty.

6.2. Procesní opatření

- vznik subjektu ve struktuře KrÚ s dostatečnou odbornou a personální kapacitou pro řízení a kontrolu systému bezpečnosti informací (možno i externě)
- definice kontrolních činností směrem k PO a ORP s předmětem dodržování pravidel bezpečnosti ICT
- vznik subjektu ve struktuře KrÚ pro správu a provoz sítě ROWANet (možno i externě) včetně centrálního HelpDesku
- vznik subjektu ve struktuře KrÚ pro centralizaci nákupu

Přínosy:

Tyto opatření umožní provozovat systém řízení bezpečnosti informací resp. ICT jako samostatnou disciplínu subjektem nezávislým na OI. Tímto je dosaženo reálné kontroly a zajištění reálné bezpečnosti. Při vzniku bezpečnostních incidentů je připraven nezávislý nástroj pro odhalení příčin a nedostatků. Nezávislost subjektu předpokládá efektivitu v jeho činnosti.

Pokud budou pravidla pro PO a ORP vymahatelná, zmíněné subjekty budou na implementaci pravidel reálně pracovat.

Vznik dvou nových subjektů (správa infrastruktury a centr.nákup) zajistí především ekonomickou výhodnost a vyšší transparentnost procesu nákupu.

Centrální nákup může pracovat s vyššími objemovými slevami, bude mít větší prostor pro komunikaci s dodavateli a dosažení slev, KrÚ získá vyšší kontrolu nad vynakládanými prostředky. Takto budou moci být definovány okruhy tzv. prověřených dodavatelů a lze takto dosáhnout i zrychlení procesu nákupu.

ROWANet je v současné době spravován OI nicméně zaslouží si, vzhledem ke svému regionálnímu významu a nárokům na správu, samostatný subjekt, který by jej spravoval a provozoval. Součástí by měla být i centrální technická podpora. Toto opatření souvisí se snahou maximalizovat počet uživatelů sítě z řad subjektů VS. Toho to lze dosáhnout pouze zkvalitněním a rozšířením služeb, které infrastruktura poskytuje, toto bohužel v současné situaci pod správou OI je velmi obtížné. Důvode je omezená kapacita OI, které je dnes vytíženo činnostmi a projekty.

Je nutno zvážit možnost externího zajištění subjektu pro správu infrastruktury, provést analytický pohled na nákladovost v obou variantách. Toto není předmětem tohoto dokumentu.

6.3. Technická opatření

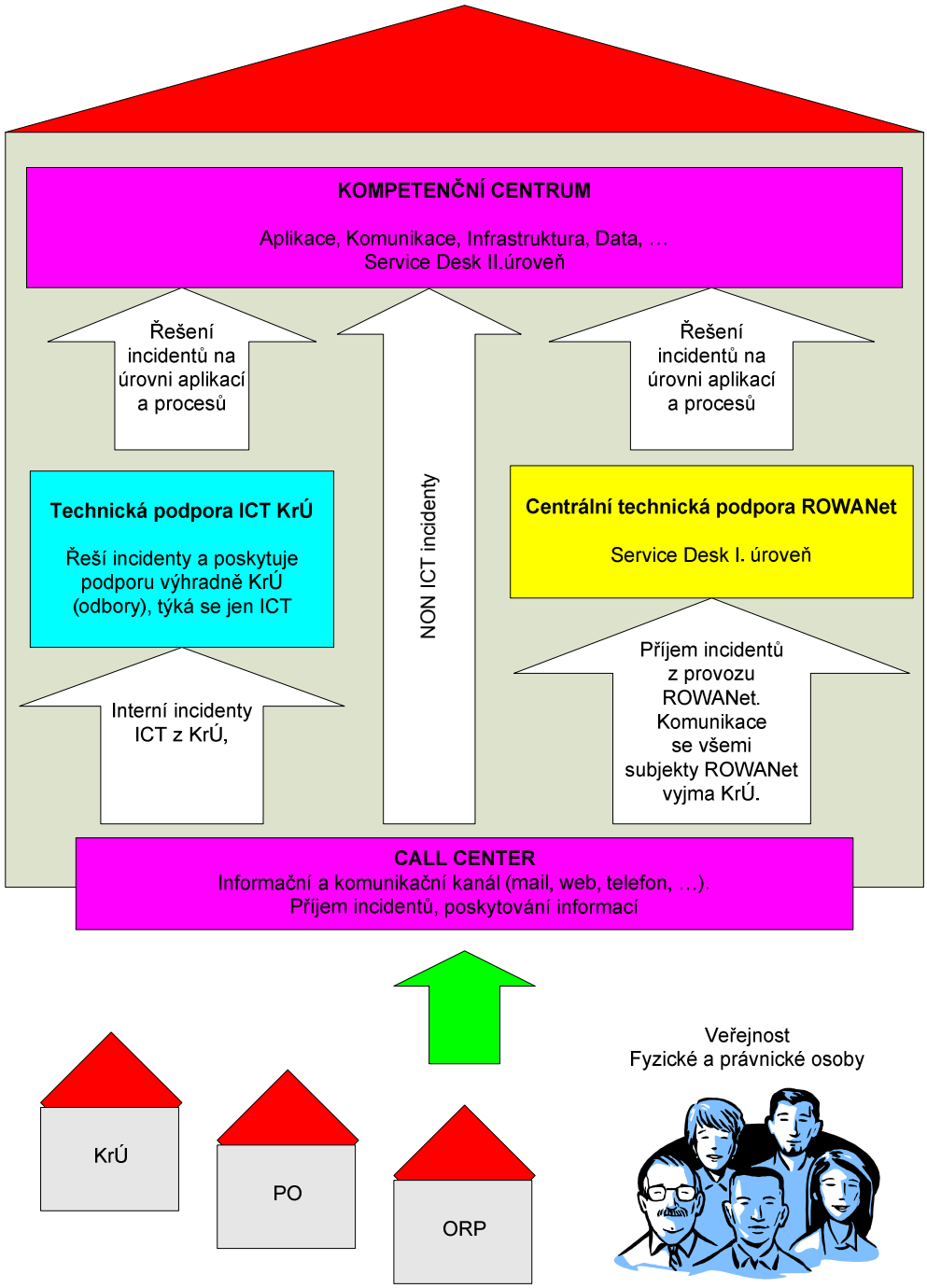
- vybudování dohledového a monitorovacího centra ROWANet včetně krajského CSIRT – Centrální technická podpora ROWANet
- vybudování pilotních instancí pro skupiny PO a ORP (vzorové implementace systému řízení bezpečnosti)

Přínosy:

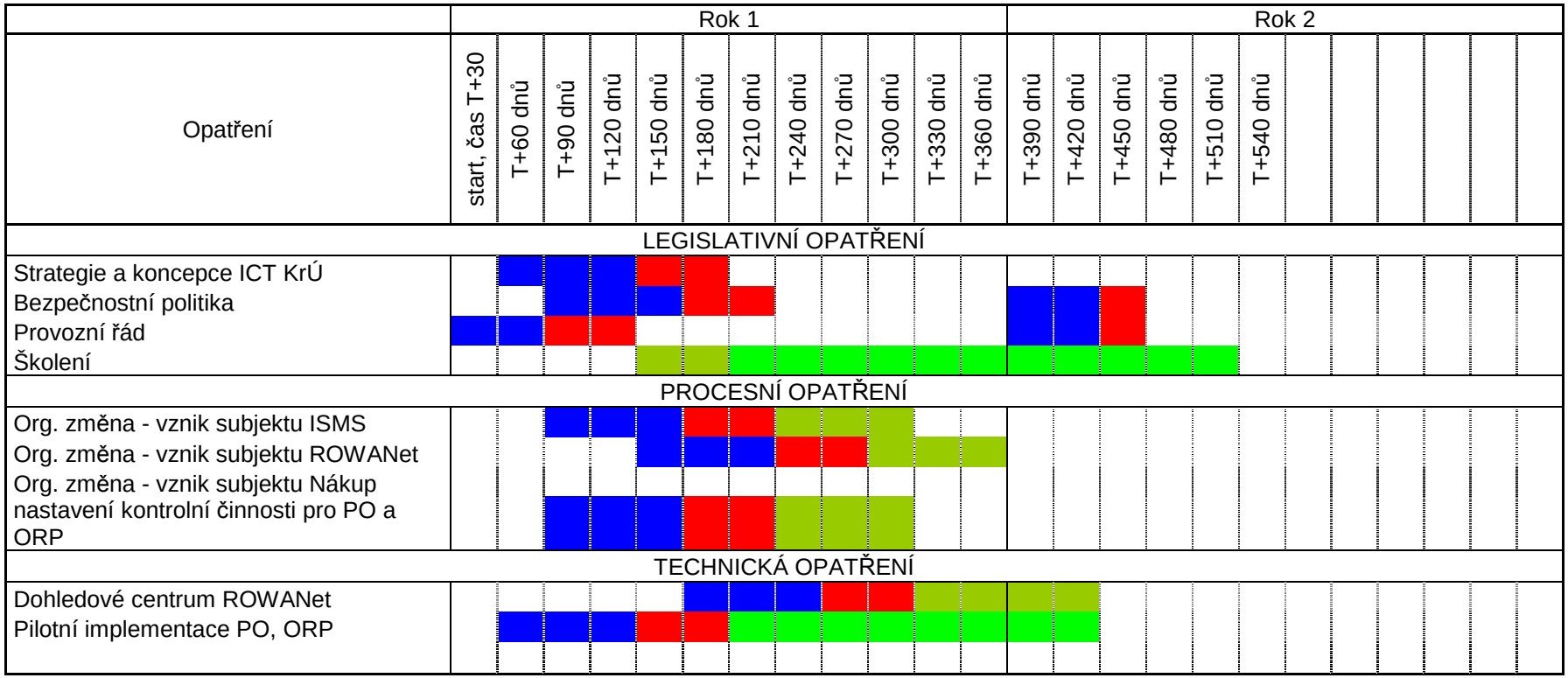
Dohledové centrum zajistí provozovateli (KrÚ) kontrolu nad infrastrukturou, chováním uživatelů a způsobu využívání, včetně vytížení. Samozřejmostí je získávání znalostí o externích a interních hrozbách a zajištění vysoké úrovně bezpečnosti. Uživatelé sítě budou mít k dispozici odbornou a dostupnou podporu a služby na standardní úrovni za přijatelné náklady.

V rámci projektů eCrime, eHealth a TC ORP je vhodné vybudovat pilotní instance – vybrané PO a ORP, kde bude nastavena vzorová úroveň bezpečnosti, tak aby bylo možno pro ostatní subjekty cílových skupin sdílet zkušenosti a poznatky. Model vzorových instancí umožní komunikaci uvnitř cílové skupiny s ohledem na její specifika a požadavky a poskytne dostatečnou znalostní základnu pro projekt „kompetenčního centra".

Schéma umístění a funkce navrženého subjektu „Centrální technická podpora ROWANet"



6.4. Návrh harmonogramu



Legenda:

příprava, zpracování
připomínky, schválení
realizace, implementace

Pozn.: Legislativní opatření je třeba provést ještě jednou formou aktualizace a zakotvení provedených změn, tak jak reálně proběhly.

Komentář k harmonogramu:

Harmonogram je navržen bez ohledu na okolní vlivy v prostředí KrÚ. Znamená to, že se jedná o optimistickou variantu, kde předpokládáme, že do projektu nevstupují žádné omezující faktory, jako například další spuštěné projekty, dovolené, fluktuace apod. tento návrh deklaruje obecnou časovou náročnost, tak aby vedení KrÚ mělo představu, že realizace změn alokuje asi dva roky. Další důležitou informací je návaznost jednotlivých opatření v blocích dle rozdělení. S bloky opatření lze vůči sobě pohybovat, ale je nutno mít na zřeteli, že musí být zachována logická kontinuita.

7. Finanční část strategie – náklady spojené s implementací strategie včetně vazeb na možné externí fondy pro financování aktivit

7.1. Náklady spojené s implementací strategie

Při stanovení finanční náročnosti vycházíme ze zkušeností z realizace obdobných projektů a obvyklých cen na trhu ICT.

Finanční hodnoty jsou svázány s navrženými opatřeními. Jednotlivé nákladové položky jsou rozděleny na přímé a nepřímé.

Nepřímé náklady – provozní náklady na personál, prostory, el. en., spotřební materiál, … atd.

Přímé náklady – nákup služeb, zboží, externích pracovníků

Tabulka: náklady na realizaci opatření

položka	náklady		
Opatření	nepřímé náklady	přímé náklady	náklady celkem
LEGISLATIVNÍ OPATŘENÍ			
Strategie a koncepce ICT KrÚ	320 000 Kč	400 000 Kč	720 000 Kč
Bezpečnostní politika	320 000 Kč	350 000 Kč	670 000 Kč
Provozní řád	80 000 Kč	Bez investice	80 000 Kč
Školení	500 000 Kč	850 000 Kč	1 350 000 Kč
PROCESNÍ OPATŘENÍ			
Org. změna - vznik subjektu ISMS	140 000 Kč	300 000 Kč	440 000 Kč
Org. změna - vznik subjektu ROWANet	140 000 Kč	300 000 Kč	440 000 Kč
Org. změna - vznik subjektu Nákup	140 000 Kč	300 000 Kč	440 000 Kč
nastavení kontrolní činnosti pro PO a ORP	240 000 Kč	150 000 Kč	390 000 Kč
TECHNICKÁ OPATŘENÍ			
Dohledové centrum ROWANet	160 000 Kč	1 000 000 Kč	1 160 000 Kč
Pilotní implementace PO, ORP	320 000 Kč	2 000 000 Kč	2 320 000 Kč
NÁKLADY CELKEM	2 360 000 Kč	**5 650 000 Kč**	8 010 000 Kč

7.2. Provozní náklady po realizaci opatření

Po ukončení realizační fáze bude nastaven rutinní provoz tří nových subjektů ve struktuře KrÚ. V níže uvedené tabulce je uveden odhad nákladů na jejich provoz. Výše ovšem není relevantní jako položka, kterou je nutno přičíst ke stávajícímu rozpočtu KrÚ jako navýšení. Z velké části se jedná o vyčlenění stávajících činností mimo stávající odbory, tudíž provozní náklady tedy stoupnou nepatrně.

Tabulka: provozní náklady po dokončení implementace

	počet pracovníků	náklad/měsíc	náklad/rok	investice/rok	celkem/rok
řízení ISMS	3	115 000 Kč	1 200 000 Kč	1 000 000 Kč	2 200 000 Kč
správa ROWANet	3	140 000 Kč	1 680 000 Kč	5 000 000 Kč	6 680 000 Kč
Centrální nákup	2	100 000 Kč	1 200 000 Kč	500 000 Kč	1 700 000 Kč
CELKEM			4 080 000Kč	6 500 000 Kč	10 580 000 Kč

7.3. Vazby na možné externí financování

Doporučujeme zaměřit pozornost na výzvy z oblasti IOP a OPLZZ. Tyto programy financování jsou orientovány na vzdělání a ICT, což jsou nedílnými faktory pro tvorbu systému bezpečnosti ICT.
Obecně lze říci, že každý projekt ICT je dotčen řešení bezpečnosti. Například výzva IOP č. 06 a 08 dávaly významný prostor pro nákup technologií pro zabezpečení TC a povýšení obecného standardu bezpečnosti ICT. V rámci své metodické činnosti může KrÚ doporučovat ORP v regionu zaměření na toto téma a poskytnout jim možnost spolupráce při budování bezpečnosti ICT v regionu.
Výzvy v rámci OPLZZ umožňují i financovat personální a procesní záležitosti. OSF-MVČR deklaruje, že bude vypsáno ještě několik tematických výzev orientovaných do vzdělávání v souvislosti s rozvojem subjektů VS.

V současnosti tedy je možno využít IOP č. 08 pro potřeby KrÚ a PO, dále IOP č. 06 pro potřeby ORP. Pro financování procesních a vzdělávacích opatření je třeba vyčkat další výzvy OPLZZ.

8. Akční plán implementace systému řízení bezpečnosti včetně doporučení k realizaci

8.1. Akční plán

8.1.1. Definice realizačního týmu a rolí členů týmu

Pro potřeby tohoto dokumentu předkládáme návrh skladby realizačního týmu, který bude plnit aktivity uvedené v Akčním plánu. Zpracovatel nemá prostor pro zjištění konkrétních osob, a proto uvede modelové role včetně kompetencí tak, aby KrÚ mohl do uvedených rolí dosadit konkrétní osoby dle možností v reálném čase. Doporučujeme, tým během realizace doplnit o pracovníky z nově vzniklých subjektů a zapojit je tak do projektu v době realizace.
Pro odpovědnost za plnění jednotlivých aktivit jsou navrženy konkrétní role, nicméně řešitelem je vždy celý tým. Pro konkrétní aktivitu je vytvořen „miniprojekt" a v rámci projektového řízení, je tým veden pro každou jednotlivou aktivitu zodpovědnou rolí (osobou).

ROLE	Oblast	Kompetence	Zkušenost
Koordinátor	Organizace, legislativa	Komunikace s vedením KrÚ, vedení projektu	Komplexní znalost KrÚ
Řízení ICT	ICT	Požadavky a nároky související s ICT	Detailní znalost ICT KrÚ
Řízení HR	Personalistika	Organizační a personální změny	Principy řízení KrÚ
Řízení kvality (administrativy)	Organizace, struktura KrÚ	Dopady do struktury řízení KrÚ	Řízení dokumentace KrÚ, auditní činnost
Řízení procesů	Organizace, struktura KrÚ	Dopady do procesů KrÚ	Řízení procesů KrÚ
Řízení legislativy	Legislativa	Dopady do interní legislativy a strategických dokumentů	Struktura interní legislativy, auditní činnost
Administrativa	administrativa	Příprava dokumentace pro realizaci jednotlivých aktivit	Interní administrativa

Aktivity – akční plán na rok 2011

Aktivita	Odpovědnost - Role
Doplnění a aktualizace dokumentu Strategie ICT pro KrÚ (včetně PO)	Řízení ICT
Strategie - schválení v orgánech KrÚ	Koordinátor
Doplnění a aktualizace dokumentu Bezpečnostní politika KrÚ	Koordinátor
Politika - schválení v orgánech KrÚ	Koordinátor
Rozpracování politiky do provozních příruček	Řízení legislativy
Rozpracování politiky KrÚ na dokumentaci pro PO a ORP	Řízení legislativy
Dopracování Provozní dokumentace a Provozního řádu	Řízení ICT
Aktualizace Katalogu služeb	Řízení ICT
Prezentace záměru KrÚ v oblasti budování systém řízení bezpečnosti ICT	Koordinátor
Promítnutí záměru do rozpracovaných projektů eHealth, eCrime	Řízení ICT
Příprava organizačních změn (procesní dopady)	Řízení procesů
Projednání organizačních změn v orgánech vedení KrÚ	Řízení kvality
Nastavení procesů a pravidel pro centrální nákup	Řízení procesů
Realizace organizačních změn (řízení ISMS, centrální nákup – personál)	Řízení HR

Analýza variant správy sítě ROWANet – výběr vhodné varianty	Koordinátor
Příprava změny subjektu pro správu sítě ROWANet	Řízení kvality
Realizace změny	Koordinátor
Zahájení procesu řízení bezpečnosti ICT v KrÚ (osvěta, úvodní skolení, nastavení procesů)	Koordinátor
Nastavení kontrolních procesů pro řízení bezpečnosti ICT	Řízení legislativy
Ověření rutinního plnění procesů pro řízení bezpečnosti ICT	Řízení kvality
Příprava pro implementaci Bezpečnostní politiky na PO (osvěta, úvodní školení managementu)	Koordinátor
Metodická spolupráce s ORP (vytvoření standardu pro TC a navržení pilotní instalace)	Řízení ICT
Kompletace katalogu služeb pro KrÚ, PO a ROWANet	Řízení ICT
Příprava pro budování Centrálního HelpDesk (nastavení procesů, dokumentace, personál)	Řízení procesů, Řízení HR
Spuštění Centrálního HelpDesk	Koordinátor
Ověřovací provoz HelpDesk (vyhodnocení, připomínky, změny)	Řízení ICT
Vypracování projektů pro pilotní implementaci bezpečnosti (PO, ORP)	Řízení ICT
Stanovení pilotních míst pro budování vzorové bezpečnosti (PO, ORP) a předložení projektů	Koordinátor
Realizace projektů (implementace spolu s TC)	Řízení ICT
Vyhodnocení dosažené úrovně bezpečnosti ICT (12/2011)	Řízení kvality
Vyhodnocení úrovně investic oproti nastaveným cílům	Řízení kvality
Aktualizace akčního plánu dle dosažených výsledků pro 2012	Koordinátor
Průběžně vzdělávací kurzy a semináře v oblasti bezpečnosti ICT.	Řízení HR

Aktivity – akční plán na rok 2012:

Aktivita	**Odpovědnost - Role**
Aktualizace strategických dokumentů dle dosažených výsledků	Řízení kvality
Aktualizace Bezpečnostní politiky dle načerpaných zkušeností	Řízení kvality
Nastavení procesu průběžných zlepšování v oblasti bezpečnosti ICT	Řízení procesů, Řízení ICT
Nastavení procesu průběžného zlepšování úrovně služeb centrálního HelpDesk	Řízení ICT
Nastavení procesu průběžného vzdělávání v oblasti bezpečnosti ICT	Řízení HR
Testovací audit dle ISO 2700x, včetně vyhodnocení	Řízení kvality
Projednání možnosti certifikace KrÚ	Koordinátor
Prezentace projektu (ISSS)	Koordinátor

8.2. Doporučení k realizaci

Během realizace navržených opatření je třeba se držet následujících doporučení, která jsou mnohokrát ověřena praxí:

- Pro obsah strategických dokumentů je vhodné zvolit méně ambiciózní tvrzení v oblasti technologií a směrovat plánovaný rozvoj ke kvalitě.
- Bezpečnostní politika nemusí být rozsáhlá a detailní ale pochopitelná a funkční.
- Konkrétní záležitosti procesů je vhodné popisovat na úrovni příruček a směrnic.
- Vždy musí být jasné kompetence.
- Norma je doporučení, ale není to dogma.
- Vykonavatel činnosti sám sebe nikdy kvalitně nezkontroluje
- Vymýšlet nové postupy je riskantní, ověřené praktiky se lépe modernizují.
- Opatření v interních aktech jsou doplněním, specifikací a výkladem platné legislativy, ne její náhradou.

- Interní legislativa slouží k tomu, aby v případě incidentu bylo jasné kdo, kde a co porušil či zanedbal nebo kde se stala chyba.
- Veškeré normativní akty před uvedením do praxe je dobré komunikovat napříč cílovými skupinami
- Nastavené procesy je dobré si otestovat se všemi vlivy
- Během realizace je nutno vést interní marketingovou kampaň (podpora vedení)
- Klíčoví lidé ve změnách se musí se změnami ztotožnit
- Udržovat rozumný poměr mezi investicemi do technických prostředků a do procesů
- Budování systému řízení bezpečnosti informací musí být provázáno se všemi činnostmi úřadu
- Každý proces musí mít nastaven kontrolní proces
- Školit, školit, školit …