PROJEKTOVÝ ZÁMĚR
Zvýšení bezpečnosti provozu informačních systémů Plzeňského kraje

Zpracovatel (zodpovědná osoba): Ing. Jiří Lohr
Ing. Eliška Pečenková

Aktualizace dokumentu - provedené revize

Verze	Autor	Datum	Revize
1.0	Lohr, Pečenková	12.06.2017	Vytvoření dokumentu

1. SHRNUTÍ

Dle zákona o kybernetické bezpečnosti č. 181/2014 Sb. v platném znění (ZoKB) provozuje Plzeňský kraj pět významných informačních systémů. K naplnění tohoto zákona je mimo jiné nezbytné realizovat sadu technických opatření, na které je možné využít podporu z dotačních prostředků Evropské unie.

1.1. Definice problému

Plzeňský kraj provozuje informační systémy, z nichž některé jsou významnými informačními systémy (VIS) dle zákona o kybernetické bezpečnosti. Jedná se o:

- Mailový server - Systém pro příjem a odesílání elektronické pošty v rámci komunikace krajského úřadu
- Integrační sběrnici - Komunikační systém, zpracovává a zajišťuje komunikaci mezi interními systémy a externím systémem - základní registry
- Spisovou službu - evidence dokumentů a spisová služba
- Webový portál kraje - Systém pro webový portál a komunikací s veřejností v rámci webového portálu
- ERP - Ekonomický informační systém pro evidenci majetku, vedení účetnictví, tvorbu rozpočtu

.U těchto informačních systémů je nutné zajistit dostupnost, integritu a důvěrnost minimálně v rozsahu, které ukládá zákon o kybernetické bezpečnosti.

1.2. Popis projektu

Realizace sady technických opatření, kterou dojde ke zvýšení zabezpečení systémů dle požadavků zákona o kybernetické bezpečnosti a souvisejících předpisů. Jedná se o implementaci nových prvků k zajištění standardů kybernetické bezpečnosti a implementaci modernizovaných systémů k zajištění standardů kybernetické bezpečnosti stávajících provozovaných významných informačních systémů. Bližší popis projektu je uveden v kapitole č. 3.

Žadatelem i příjemcem podpory bude Plzeňský kraje.

Zdroj spolufinancování:

Operační program:	06 Integrovaný regionální operační program
Prioritní osa:	06.3 Dobrá správa území a zefektivnění veřejných institucí
Investiční priorita:	06.3.05 Posilování aplikací v oblasti IKT určených pro elektronickou veřejnou správu, elektronické učení, začlenění do informační společnosti, elektronickou kulturu a elektronické zdravotnictví
Specifický cíl 3.2	Zvyšování a efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT
Číslo výzvy:	10 – kybernetická bezpečnost.

1.3. Posouzení projektu

Hlavním přínosem projektu bude naplnění povinností kladené zákonem a souvisejícími nařízeními za finančního přispění Evropské unie.

2. DEFINICE PROBLÉMU

Zvýšení dostupnosti, integrity a důvěrnosti Plzeňským krajem provozovaných významných informačních systémů.

2.1. Popis problému

Plzeňský kraj provozuje informační systémy, které dle zákona o kybernetické bezpečnosti naplňují definici významných informačních systémů (integrační sběrnice, mailový server, webový portál, spisovou službu, ERP).

Tyto informační systémy, jejichž provozovatelem je Plzeňský kraj, byly nahlášeny Národnímu bezpečnostnímu úřadu (NBÚ).

Platná legislativní opatření kladou nároky na zajištění odolnosti významných informačních systémů veřejné správy proti kybernetickým hrozbám. Projektem budou realizovány technická opatření vedoucí k zabezpečení významných informačních systémů Plzeňského kraje.

2.2. SWOT analýza

Problematice bezpečnosti je odborem informatiky dlouhodobě věnovaná nadstandartní pozornost. Zákon o kybernetické bezpečnosti a související vyhlášky upravují práva a povinnosti orgánů veřejné moci v oblasti kybernetické bezpečnosti. Pro naplnění těchto zákonných ustanovení je nezbytné přistoupit k obměně části řešení i k pořízení nových řešení.

SWOT analýza bude v případě schválení projektového záměru Radou Plzeňského kraje zpracována jako součást studie proveditelnosti. Uvedené body jsou pouze ilustrativní, nicméně realizace projektu je nezbytná i bez získání podpory pro spolufinancování.

Silné stránky	**Slabé stránky**
• Zvýšení zabezpečení provozovaného prostředí • Naplnění zákonných požadavků	• Pro část navrženého řešení nejednoznačnost řídících dokumentů
Příležitosti	**Hrozby**
• Získání finančních prostředků na spolufinancování z dalších zdrojů (EU)	• Nezískání podpory spolufinancování • Nezpůsobilost části výdajů • Podpora vybraných druhů zařízení s ohledem na dobu udržitelnosti projektu

3. POPIS PROJEKTU

Opatření významných informačních systémů Plzeňského kraje (integrační sběrnice, mailový server, webový portál, spisovou službu, ERP) budou naplněny dvojím způsobem:

- Implementace skupinových opatření pro informační systémy
- Implementace jednotlivých opatření pro informační systémy
- Implementace opatření pro klienty (uživatele informačních systémů)

Skupinová opatření

Vybudování vysoce dostupného uzlu pro významné informační systémy Plzeňského kraje (integrační sběrnice, mailový server, spisovou službu, ERP VIS) prostřednictvím dvou geograficky oddělených serverových systémů, které v případě výpadku jedné lokality zajistí potřebnou dostupnost významných informačních systémů v druhé lokalitě. Toto řešení je použito pro systémy provozované ve vnitřní síti organizace. Webový portál je vyřešen umístěním v demilitarizované zóně.

Jednotlivá opatření

Mailový server Plzeňského kraje = systémy které zajišťují bezproblémový provoz elektronické pošty. V současné době je mailový server provozován na platformě MS Exchange 2010 se zabezpečením formou antispamové a antivirové brány od jedné společnosti. Pro zvýšení bezpečnosti těchto systémů bude projektem realizováno pořízení dvou Exchange 2016 nodů, které bude doplněno o zabezpečení další antispamovou a antivirovou bránou. Dalším opatřením bude zvýšení dostupnosti pro poštovní klienty, kteří přistupují k poštovním schránkám prostřednictvím Internetu.

Webový portál – v současné době provozujeme základní přístup k tomuto informačnímu systému prostřednictvím dvou zařízení, u kterých je nutné vyměnit komponenty (konec záruční doby). Realizací projektu bude zajištěna náhrada části stávajícího řešení. U tohoto systému bude projektem dále řešeno i zvýšení bezpečnosti na L7 vrstvě.

Opatření pro klienty

Všichni uživatelé sítě Plzeňského kraje mají přístup minimálně k významnému informačního systémů mailový server. Z tohoto důvodu je nutné zvyšovat bezpečnost těchto uživatelů. Tímto projektem bude dále zvýšena bezpečnost přístupu k Internetu výměnou stávajícího řešení (stávající řešení bude do cca 2 let zastaralé a nebude výrobcem nadále podporováno).

Dalšími opatřeními jsou:

- zvýšení verze typu operačního systému, který poskytuje vyšší zabezpečení z provozu aplikací
- zvýšení bezpečnosti připojení uživatelských stanic do sítě organizace.

3.1. Cíle projektu

č.	cíl	měřitelné parametry	podmínky realizace/omezení
1.	Nové prvky (systémy) k zajištění standardů kybernetické bezpečnosti	počet realizovaných technických bezpečnostních opatření podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti	
2.	Modernizované prvky (systémy) k zajištění standardů kybernetické bezpečnosti	počet realizovaných technických bezpečnostních opatření podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti	

3.2. Organizační zajištění projektu

Pro oblast bezpečnosti je ředitelem Krajského úřadu Plzeňského kraje ustanoveno Bezpečnostní fórum. Jedná se orgán dle ČSN ISO/IEC 27001, který je složen ze zástupců vedení úřadu a jednotlivých odborů a řeší otázky informační bezpečnosti (související vnitřní předpis: Provozní řád informačního systému Krajského úřadu Plzeňského kraje Ř-2/2009).

V roce 2016 bylo ustanoveno Fórum pro Kybernetickou bezpečnost, které je složeno zástupců vedení úřadu, vybraných odborů a správců významných informačních systémů (související předpis: zákon o kybernetické bezpečnosti č. 181/2014 Sb. v platném znění). Tento orgán bude gestorem (řídícím výborem) projektu.

Vedení projektu:

- náměstek hejtmana pro oblasti regionální rozvoj, fondy EU a informatiku,
- odbor informatiky KÚPK (3)

Projektový (realizační) tým:

- odbor informatiky KÚPK (3)

Zajištění administrace projektu:

- odbor fondů a programů EU (1)

Příprava projektové žádosti:

- odbor fondů a programů EU ve spolupráci s odborem informatiky,

Příprava studie proveditelnosti:

- dodavatelsky

Administrace veřejných zakázek:

- odbor informatiky KÚPK, externě

3.3. Rámcový harmonogram a milníky projektu

Etapy řešení	Termín zahájení	Termín ukončení
Předprojektová:		
Příprava studie proveditelnosti, projektové žádost a souvisejících dokumentů	**Červen 2017**	**Říjen 2017**
Projektová:		
Zpracování technických specifikací dílčích řešení - průběžné	**Červen 2017**	**Březen 2018**
Realizace výběrových řízení - průběžná	**Srpen 2017**	**Květen 2018**
Implementace, testování, penetrace - průběžně	**Září 2017**	**Listopad 2018**
Poprojektová:		
Udržitelnost projektu	**Listopad 2018**	**Listopad 2023**

3.4. Předpokládaný rozpočet projektu a návrh možného způsobu financování

Celkové náklady projektu: *40 000 000 Kč včetně DPH*

Způsobilé výdaje: *15 000 000 Kč včetně DPH*

Nezpůsobilé výdaje: *25 000 000 Kč včetně DPH*

Dotace (90 % způsobilých výdajů): *13 500 000 Kč včetně DPH*

Vlastní zdroje žadatele: *26 500 000 Kč včetně DPH*

Zdroje financování:

- Předprojektová fáze: Rozpočet Plzeňského kraje
- Projektová fáze: Rozpočet Plzeňského kraje – Individuální projekty, iROP 10 *Pro rok 2017 zahrnuty požadavky na rozšíření infrastruktury v Individuálních projektech – námětech ve výši 10 mil. Kč.. Pro následující roky budou finanční prostředky nárokovány v Individuálních projektech (TAS)*
- Poprojektová fáze: Rozpočet Plzeňského kraje – Individuální projekty

Detailní rozpočet, včetně rozpadu do jednotlivých let, bude zpracována jako součást studie proveditelnosti.

4. POSOUZENÍ PROJEKTU

4.1. Strategický soulad

Realizací projektu budou naplněny vybrané povinnosti zákona o kybernetické bezpečnosti ve vztahu k významným informačním systémům, jejichž provozovatelem je Plzeňský kraj.

4.2. Analýza dopadů na organizaci

Přínosy: implementace sady technických opatření pro zvýšení zabezpečení systémů dle požadavků zákona o kybernetické bezpečnosti a souvisejících předpisů

Závazky: zajištění udržitelnosti projektu

4.3. Finanční analýza přínosů a nákladů

Ve vztahu k projektu není v této fázi přípravy možné přesné vyčíslení. Investice do zabezpečení IT infrastruktury a informačních systémů vyžadují systémový přístup - jsou významné a nejsou jednorázové. Jsou spojeny s pravidelnými poplatky, které nejsou uznatelnými výdaji projektu. V tomto případě se jedná o splnění povinnosti dané platnými legislativními předpisy orgánu veřejné moci, které nebude omezeno jen dobou udržitelnosti projektu.

4.4. Analýza alternativních možností

Realizace projektu je nezbytná i bez získání podpory pro spolufinancování. Získáním podpory z výzvy 10 – kybernetická bezpečnost bude zajištěno kofinancování způsobilých výdajů projektu ve výši 90% (Evropská unie 85%, státní rozpočet 5%).