STUDIE PROVEDITELNOSTI PRO PROJEKT „BEZPEČNOST KOMUNIKAČNÍ INFRASTRUKTURY“

PRŮBĚŽNÁ VÝZVA Č. 10

Zpracovatel: **ALEF NULA**
Se sídlem: U Plynárny 1002/97, 101 00 Praha 10
IČ: 61858579
Zastoupen: Ing. Milan Zinek, předseda představenstva

Obsah

Seznam zkratek a pojmů

CAF	Common Assesment Framework (společný hodnotící rámec)
CBA	Cost Benefit Analysis (analýza nákladů a přínosů)
CF	Cash flow (peněžní tok)
ČR	Česká republika
DB	Databáze
DNS	Domain Name Server (hierarchický systém doménových jmen)
EU	Evropská unie
FIRR	Finanční vnitřní míra výnosnosti
FRR	Vnitřní výnosové procento
FTP	File Transport Protocol (protokol aplikační vrstvy)
FW	Firewall – Bezpečnostní zařízení zabezpečující provoz mezi sítěmi
GB	Gigabyte
http	Internetový protokol
HW	Hardware
ICT	Informační a komunikační technologie
IDS	Intrusion Detection System (detektory rozpoznávající napadaní či pokusy o napadení koncových stanic)
IP	Internet Protocol (datový protokol)
IPS	Intelligent Protection System (inteligentní systém ochrany)
IROP	Integrovaný regionální operační program
IS	Informační systém
ITIL	Standard pro řízení IT služeb
KB	Kybernetická bezpečnost
KIVS	Komunikační infrastruktura veřejné správy
KÚ	Krajský úřad
LAN	Local Area Network (lokální síť)
Maintenance	Údržba, podpora
Malware	Zákeřný software
Mbps	Megabit za sekundu
MMR	Ministerstvo pro místní rozvoj
Model OSI	Norma pro standardizaci počítačových sítí
MV ČR	Ministerstvo vnitra České republiky
NTP	Network Time Protocol (služba přesného času)
OK	Pardubický kraj
open source	SW s otevřeným zdrojovým kódem
ORP	Obec s rozšířenou působností
P2P	Peer to peer (druh architektury počítačových sítí)
PO	Příspěvková organizace
Redundance	Prostředek ke zvyšování spolehlivosti a odolnosti proti chybám

RFC	Standarty popisující internetové protokoly, systémy atd.
RU	Prostor v slaboproudém rozvaděči typu rack pro fyzickou instalaci zařízení, např. serveru
ŘO IOP	Řídící orgán integračního operačního programu
Single point of failure (SPOF)	Část, slabé místo systému, při jejíž poruše systém přestává pracovat
SLA	Service level agreement (dohoda o garantované úrovni kvality služeb)
SMPT	Server odchozí pošty
SNMP	Simple Network Management Protocol (součást sady internetových protokolů)
SP	Studie proveditelnosti
SW	Software
Switch	Přepínač
TC	Technologické centrum
VMware	Vizualizační SW
WAN	Wide Area Network (počítačová síť, která pokrývá rozlehlé geografické území)
Workflow	Průběh pracovní operace, technologický postup
XML	Rozšiřitelný značkovací jazyk
ŽP	Životní prostředí

Seznam tabulek

Seznam obrázků

2. Úvodní informace

Studie proveditelnosti byla zpracována dle metodiky – přílohy č. 2 Specifických pravidel pro 10. výzvu IROP a zpracovává záměr výrazného zvýšení bezpečnosti informačních systémů krajského úřadu vycházející ze zákona č.181/2014 Sb. o kybernetické bezpečnosti. Východiskem pro zpracování studie proveditelnosti byl dokument „Strategický rámec rozvoje veřejné správy ČR pro období 2014-2020“ zpracovaný Ministerstvem vnitra, odborem strategického rozvoje a koordinace veřejné správy, a to především okruh číslo 7. Kybernetická bezpečnost.
Rada Pardubického kraje se dlouhodobě zabývá bezpečností informačních systémů Krajského úřadu a rozhodla o zpracování studie proveditelnosti pro výzvu č. 10, prioritní osa 3 - Dobrá správa území a zefektivnění veřejných institucí, specifický cíl 3.2 - Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů ICT, tedy i pro oblast kybernetické bezpečnosti Pardubického kraje.

2.1. Základní informace o zpracovateli

Obchodní jméno	**ALEF NULA, a.s.**
Sídlo	U Plynárny 1002/97, 101 00 Praha 10
IČ	61858579
DIČ	CZ61858579
Členové zpracovatelského týmu, jejich role a kontakty	- Michal Zedníček, koordinátor, +420 602 578 443, Michal.Zednicek@alef.com - Ing. Petr Vácha, technický architekt projektu, +420 604 220 206, Petr.Vacha@alef.com - Mgr. Tomáš Poledno, projektový manažer projektu, +420 724 815 483, Tomas.Poledno@alef.com - Ing. Robert Belovský, zodpovědný za cenovou část nabídky, Key Account Manager, +420 702 154 276, Robert.Belovsky@alef.com - Ing. Andrea Jonštová, zodpovědná za finanční část nabídky, +420 603 179 117, Andrea.Jonstova@alef.com
Datum vypracování:	7.6.2017

Tabulka 1 Informace o zpracovateli

Tento dokument byl zpracován společností Alef Nula, a.s. v úzké spolupráci s určenými zaměstnanci žadatele a jako doplňující zdroj informací sloužily dokumenty stávajícího stavu dodané žadatelem.

.

3. Základní informace o žadateli

Obchodní jméno	Pardubický kraj
Sídlo	Komenského nám. 125, 532 11 Pardubice
IČ	70892822
DIČ	CZ70892822
Statutární zástupce	JUDr. Martin Netolický, Ph.D., hejtman Telefon: +420 466 026 114 E-mail : martin.netolicky@pardubickykraj.cz
Kontaktní osoba	Ing. Roman Borkovec, vedoucí odboru informatiky Telefon: +420 466 026 180 E-mail: roman.borkovec@pardubickykraj.cz
Nárok na odpočet DPH na vstupu ve vztahu ke způsobilým výdajům projektu (Ano x Ne)	NE
Název projektu	Bezpečnost komunikační infrastruktury

Tabulka 2 Informace o žadateli

Žadatel splňuje definici oprávněného příjemce pro příslušný specifický cíl a výzvu.

4. Charakteristika projektu a jeho soulad s programem

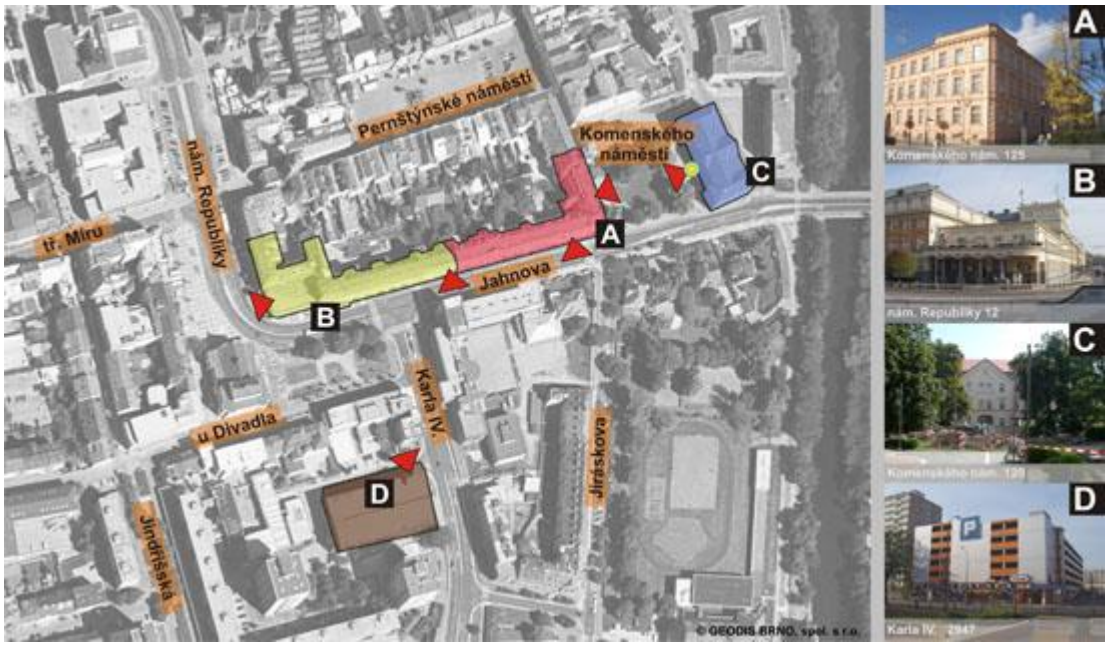
4.1. Místo realizace projektu.

Místem realizace projektu jsou prostory a objekty Krajského úřadu Pardubického kraje, které jsou v jeho vlastnictví a nachází se v krajském městě Pardubice:

- Komenského náměstí č.p. 125 – budova A
- Náměstí republiky č.p. 12 - budova B
- Komenského náměstí č.p. 120 – budova C

Pozn.: Budova D zobrazená na obr. 1 není předmětem předkládaného projektu.

Obrázek jejich polohy:



Obrázek 1 – Místa realizace projektu

4.2. Popis cílových skupin projektu.

Cílovými skupinami projektu Bezpečnosti komunikační infrastruktury je Krajský úřad Pardubického kraje a jeho zaměstnanci. Výsledný projekt a bezpečnostní opatření v něm navržená budou určeny mimo jiné pro tyto cílové skupiny:

- Zaměstnanci Krajského úřadu Pardubického kraje
- Zaměstnanci organizací zřizovaných Pardubickým krajem
- Občané
- Fyzické i právnické osoby (podnikatelé)

4.3. Popis cílů a výsledků projektu a jejich vztahu k naplňování SC 3.2 a podporovaných aktivit

Cílem tohoto projektu je zajistit soulad KÚ Pardubického kraje jako správce významného informačního systému (VIS) s požadavky ZKB a prováděcí vyhlášky. Technická opatření navrhovaná touto studií budou napomáhat, nebo

přímo řešit soulad KÚ s požadavky zákona a předcházet tak hrozbě kybernetických/bezpečnostních incidentů, jakož i možným sankcím ze strany NBÚ. Takže výsledkem projektu je posílit ochranu informačních a komunikačních systémů žadatele před kybernetickými útoky.

Vlastníkem projektu „Bezpečnost komunikační infrastruktury" je Pardubický kraj (viz kapitola **3** „Základní údaje o žadateli"), který je současně i žadatelem o dotaci v rámci Integrovaného regionálního operačního programu.

Pardubický kraj bude v případě uskutečnění projektu také vlastníkem veškerých zařízení, HW, SW komponent ICT infrastruktury a aplikací pořízených v průběhu realizace, což bude výstupem tohoto projektu.

Vzhledem k rostoucí civilizační závislosti na ICT je kladen velký důraz na zajištění kybernetické bezpečnosti krajského úřadu. Hlavním výsledkem projektu je zavedení prvků pro ochranu důvěrnosti, integrity a dostupnosti informací ve správě úřadu. Projekt si klade za cíl vybrat a implementovat bezpečnostní prvky sloužící k uvedení v soulad se **Strategickým rámcem rozvoje veřejné správy České republiky pro období 2014 – 2020** schváleným usnesením Vlády České Republiky ze dne 27. srpna 2014 č. 680 (dále jen Rámec), konkrétně strategickým cílem 3: **Zvýšení dostupnosti a transparentnosti veřejné správy**, který reaguje na zvyšující se potřebu řešení kybernetické bezpečnosti a váže se na realizaci jediného specifického cíle, kterým je **dobudování informačních a komunikačních systémů veřejné správy a realizace bezpečnostních opatření podle Zákona o kybernetické bezpečnosti České Republiky 181/2014 Sb.**, (dále jen ZKB) prostřednictvím rozvoje využití a kvality systémů ICT. Úřad jako správce „Významných informačních systémů" je povinen naplnit požadavky dané platným zněním ZKB a dodržet všechny parametry vyžadované vyhláškou č. 316/2014 Sb.

Jako stěžejní pro zajištění souladu byla identifikována tato opatření a prvky k zajištění bezpečnosti. Níže uvedená tabulka nám uvádí vazbu navržených opatření na paragrafy vyhlášky 316/2104 Sb.:

Navržená opatření a bezpečnostní řešení	*§ vyhlášky 316/2014*
Provedení GAP analýzy	**§15**
Implementace správy privilegovaných uživatelů a účtů	**§11, §18, §21**
Doplnění VPN brány	**§17, §18, §25**
Zajištění redundance optických tras pro přístupové switche	**§26**
Doplnění přístupových přepínačů	**§17, §18, §19, §22, §25, §26**
Doplnění HW Datového centra o servery a pole	**§26**
Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě	**§18, §19**
Centrální logovací nástroj	**§21**
Implementace vysoké dostupnosti pro [redacted]	**§26**
Implementace řešení pro monitorování toků	**§20, §22**
Doplnění redundantní [redacted] proxy	**§17, §20, §26**

Rozšíření [redacted] o SANDBOX	**§20**
Implementace Webového aplikačního firewallu a Loadbalanceru	**§22, §24, §26**
Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS	**§21**
Doplnění konektoru [redacted] pro úložiště elektronických dokumentů	**§25**
Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů	**§18**
Rozšíření stávajícího dohledového centra [redacted]	**§26**
Implementace testovacího centra	**§24**
Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management	**§24**

Tabulka 3 - Vazba navržených opatření na paragrafy vyhlášky 316/2104 Sb.

Jak je vidět výše, navrhovaná opatření a bezpečnostní prvky významně pomohou zajistit soulad krajského úřadu mimo jiné s těmito paragrafy vyhlášky 316/2014 sb.:

- §15 - Kontrola a audit kybernetické bezpečnosti
- §17 - Nástroj pro ochranu integrity komunikačních sítí
- §18 - Nástroj pro ověřování identity uživatelů
- §19 - Nástroj pro řízení přístupových oprávnění
- §20 - Nástroj pro ochranu před škodlivým kódem
- §21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- §22 - Nástroj pro detekci kybernetických bezpečnostních událostí
- §23 - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- §24 - Aplikační bezpečnost
- §25 - Kryptografické prostředky
- §26 - Nástroj pro zajišťování úrovně dostupnosti

4.4. Problémy, které má realizace projektu vyřešit

Problémem, který vyřeší realizace projektu „Bezpečnost komunikační infrastruktury", je především nedostatečná úroveň bezpečnosti stávajících ICT systémů KrÚ Pk před možnými kybernetickými útoky. Tato hrozba se v našem digitálním světě stále zvyšuje, a proto je zde i legislativa v podobě ZKB a prováděcí vyhlášky. Navrhovaná technická

opatření v této studii budou napomáhat nebo přímo řešit soulad KÚ s požadavky zákona a předcházet tak hrozbě kybernetických/bezpečnostních incidentů, jakož i možným sankcím ze strany NBÚ. A to je druhý problém, který realizace projektu vyřeší. Nedostatečná úroveň v souladu s požadavky kybernetické bezpečnosti ICT je popsána v kapitole 5 Podrobný popis projektu 5.1.

4.5. Popis vazeb na realizované/zrealizované či plánované projekty / investiční akce

Realizace technických opatření navržených v této studii navazuje na předchozí projekt žadatele z výzvy č. 08 Integrovaného operačního programu "**Technologické centrum Pardubického kraje"** a na projekt z výzvy č. 19 „**Bezpečnostní infrastruktura technologického centra Pardubického kraje**". Technická opatření navržená v rámci řešení doplňují, nebo rozšiřují funkcionalitu stávajících ICT systémů tak, aby naplňovala požadavky definované zákonem o kybernetické bezpečnosti.

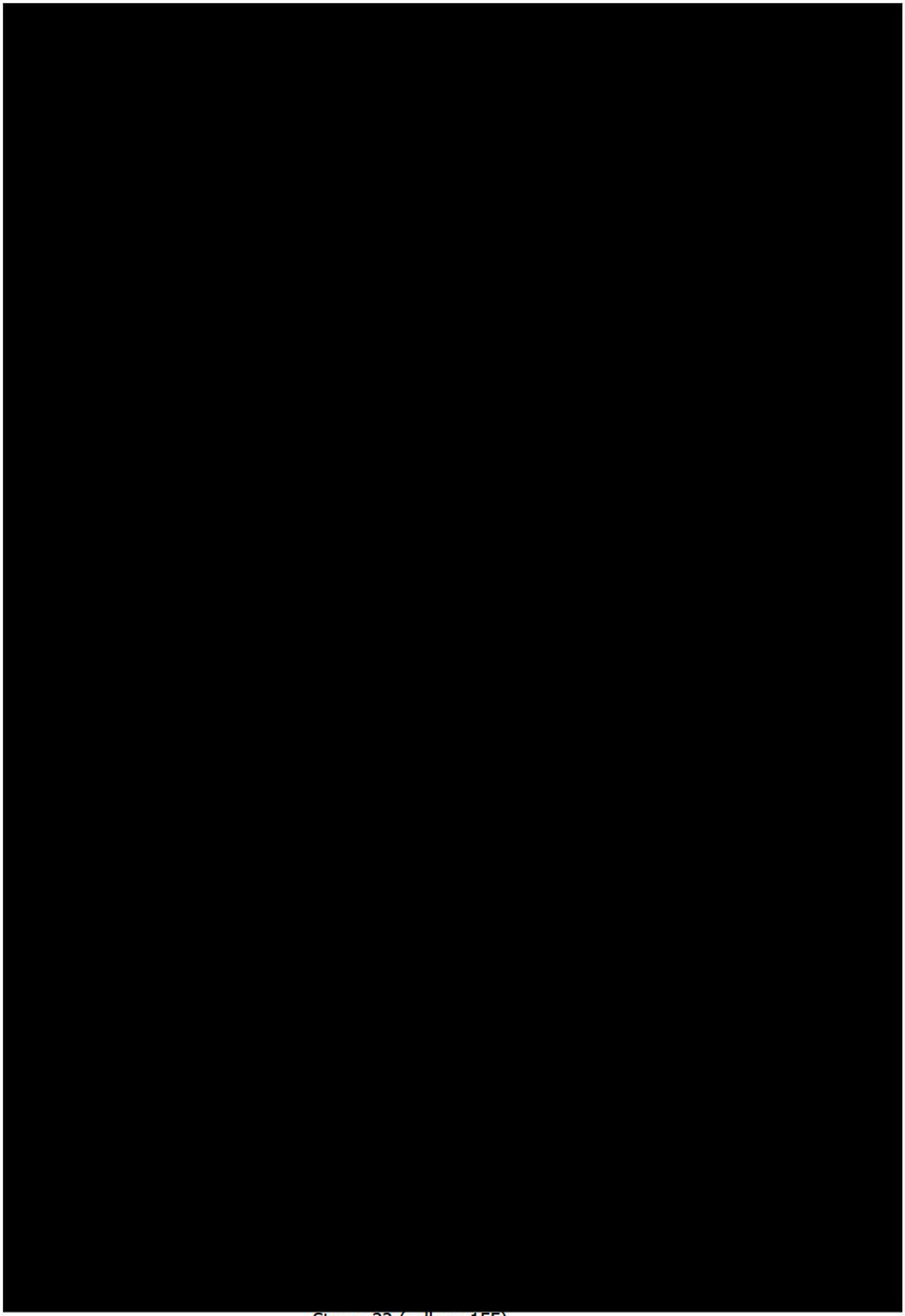
Detaily jednotlivých vazeb řešení jsou popsány v kapitole 5 Podrobný popis projektu 5.1.

5. Podrobný popis projektu

5.1. Výchozí stav – popis výchozí situace

Pardubický kraj je doménová síť využívaná úředníky a zaměstnanci Krajského úřadu. Síť je tvořena několika informačními systémy. Ty slouží buď pro vnitřní provoz přenesené a samostatné působnosti, nebo jsou celé či částečně publikované jako služba veřejnosti vně do internetu. O správu, provoz a bezpečnost informační a komunikační infrastruktury se stará oddělení informatiky Pardubického kraje. Rozhodování a jednání oddělení informatiky je dáno procesními kroky v souladu s platnou certifikací ISO 27001:2013, dále nově v souladu s platným zněním zákona č. 181/2014 Sb. O kybernetické bezpečnosti, a to včetně kybernetické ochrany významného informačního systému (VIS) definovaného ve vyhlášce č. 317/2014 Sb.

Současný stav zabezpečení sítě lze označit za ne zcela vyhovující, což lze dokumentovat neshodou s některými požadavky zákona o kybernetické bezpečnosti. Pracovníci IT oddělení si tuto situaci uvědomují a identifikovali následující rizikové oblasti, které zároveň popisují výchozí stav projektu:



[redacted]

Stávající stav páteřní optické datové sítě:

[redacted]

5.1.1. Výčet informačních a komunikačních systémů, které spravuje žadatel

Následující systémy spravuje žadatel.

5.1.1.1. Významný informační systém (VIS)

Pardubický kraj na základě určení dopadových kritérií určil integrovaný informační systém GINIS jako významný

informační systém dle zákona č. 181/2014 Sb. a nahlásil jej Národnímu bezpečnostnímu úřadu (NBÚ). Informační systém byl tak zapsán do novely vyhlášky č. 317/2014 Sb. jako VIS:

PČ	*Název VIS*	*Popis*
107	**Integrovaný informační systém GINIS**	Modulární systém GINIS společnosti Gordic. Pokrývá oblasti rozpočtu, účetnictví, majetku, dotace, styk s bankami, smlouvy, spisovou službu a další moduly související s provozem úřadu

GINIS je souhrný název pro cca 50 samostatných aplikačních modulů spojených do jedné programové platformy. V jednotlivých modulech integrovaného informačního systému pracuje každodenně přes 95 % uživatelů sítě Pardubického kraje a tento systém zasahuje do všech technických aktiv infrastruktury Pardubického kraje. Jako hlavní aktivum jsou na jeho provoz kladeny vysoké nároky dostupnosti, integrity dat a důvěryhodnosti obsahu a procesů v něm vytvořených. Ochrana se týká i infrastruktury, na které tento systém pracuje.

5.1.1.2. Kritická informační infrastruktura (KII)

Pardubický kraj nespravuje ani nezabezpečuje žádný ze systémů KII

5.1.1.3. Informační a komunikační systémy (IS/KS)

Infrastruktura Pardubického kraje je tvořena kromě VIS i dalšími systémy tvořícími platformu pro pracovníky ve veřejné správě na straně vnitřní, dále občany a další orgány veřejné moci na straně systémů zveřejněných vně do internetu jako online služby. Všechny níže zmíněné systémy by měla zabezpečit navržená opatření uvedená v této studii:

Název systému	*Typ*
Informační systém Krajského úřadu Pardubického kraje	IS
Emailový systém	KS
Webový portál Pardubického kraje	IS
Formulářový systém sběru dat z obcí	IS
Sběrové ekonomické výkazové automaty	KS
Hostovaná spisová služba	IS
Krajské digitální úložiště	IS
GIS mapové servery	IS
ISZR kukátko	IS

Tabulka 4 - Přehled IS/KS vybraných pro pokrytí navrženými opatřeními

- **Informační systém Krajské úřadu Pardubického kraje** - informační systém spojený z několika aplikací běžné denní agendy úředníků a zaměstnanců. Systém doplňuje svými funkcemi VIS GINIS a stejně jako on spolupracuje i s informačními systémy státu (ISZR, JIP/KAAS)
- **Emailový systém** – komunikační systém úřadu je veden jako jedno z primárních aktiv úřadu. I přes fungující systém datových schránek je to stále nejrozšířenější médium pro komunikaci občana a komerčních subjektů s úřadem nebo opačně.
- **Webový portál kraje (www.pardubickykraj.cz)** – portál je hlavním informačním médiem spojujícího úřad s občanem. Z hlediska důvěryhodnosti a dostupnosti informací je tak veden jako jedno z primárních aktiv.

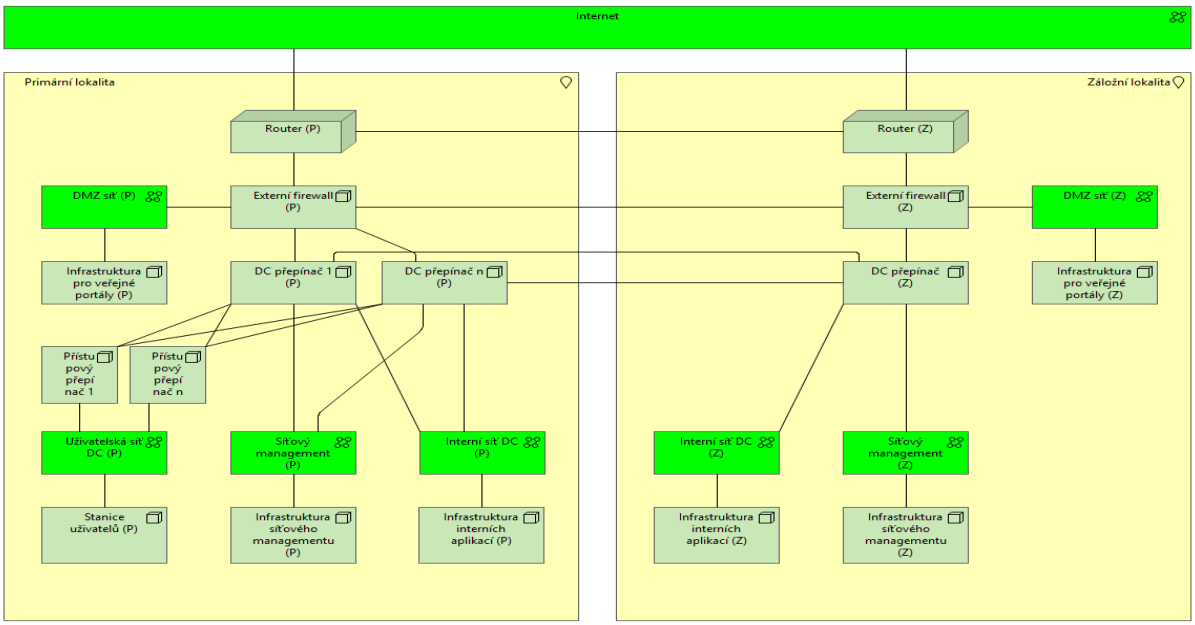
- **Formulářový systém sběru dat z obcí** – informační systém spolupracující se starosty všech obcí Pardubického kraje. Systém shromažďuje kontaktní informace, které po ověření jsou k dispozici jednotlivým agendám úřadu.
- **Sběrové ekonomické výkazové automaty** – automatický komunikační systém spojující na jedné straně obce a organizace veřejné správy, na druhé straně Centrální systém účetních informací státu (CSÚIS). Systém data přijímá, kontroluje a po kompletaci zasílá na CSÚIS.
- **Hostovaná spisová služba** – informační systém spisové služby plně zveřejněný vně úřadu využívaný zřizovanými organizacemi Pardubického kraje. Systém spolupracuje s dalšími systémy, jako jsou například základní registry.
- **Krajské digitální úložiště** – informační systém umožňující identifikaci osoby, která využije úložiště pro datovou komunikaci z internetu. Systém slouží vedle webového portálu jako nástroj výměny dat velké velikosti nebo vyššího zabezpečení.
- **GIS mapové servery** – informační systém prezentující mapové podklady občanům a organizacím. Tvorba mapových podkladů včetně doplňujících metadat je jedna z činností oddělení informatiky Pardubického kraje.
- **ISZR kukátko** – informační systém umožňující zabezpečený přístup do systému základních registrů a vyčítání informací nutných k přenesené i samostatné působnosti úřadu. Systém tak naplňuje povinnosti kladené na úřad platnou legislativou.

5.1.2. ICT vybavení Pardubického kraje

Síť Pardubického kraje je postavená na technologické platformě MS Windows. Autentifikace a autorizace probíhá vůči doménovým kontrolerům MS Active Directory s řízením koncových stanic přes Group Policy (GPO). Infrastruktura aktivních prvků je postavena na technologiích firmy Cisco. Primárním operačním systémem koncových stanic i serverového vybavení je MS Windows. Odbornost a kvalifikace administrátorů je soustředěna právě na tyto oblasti.

Infrastruktura je **bez výjimky** nosnou platformou **všech** informačních a komunikačních systémů Pardubického kraje včetně významného informačního systému a je součástí nejvyššího zabezpečení. Je tak vnímána i v oblasti kategorizace rizik. Nejvyšší míra zabezpečení je hlavně koncentrována na tři datacentra. Dvě datacentra jsou technologická, třetí je primárně komunikační. Jednotlivé prvky infrastruktury jsou tak zároveň vedeny jako technická aktiva a navrhovaná nápravná opatření jejich bezpečnost výrazně navyšují:

- Servery – (VIS, IS, KS)
- Datová úložiště – (VIS, IS, KS)
- Optická a metalická infrastruktura - (VIS, IS, KS)
- Síťové prvky – (VIS, IS, KS)
- Koncová zařízení – (VIS, IS, KS)
- Datová centra (VIS, IS, KS)
- Ostatní režimová pracoviště (IS, KS)



Obrázek 3 - Popis současného stavu řešení

5.1.3. Systémy určené k ochraně utajovaných skutečností dle zákona č. 412/2005 Sb

Žádný se systémů Pardubického kraje zde uvedených, ani jejich části netvoří rámec systémů určených k ochraně utajovaných skutečností dle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti (ISOUI).

5.2. Popis vazby projektu na Strategický rámec rozvoje veřejné správy a jeho implementační plány a projektové okruhy

Projekt plně reflektuje **Strategický rámec rozvoje veřejné správy České republiky pro období 2014 – 2020** schváleným usnesením Vlády České Republiky ze dne 27. srpna 2014 č. 680 (dále jen Rámec), implementační plán pro strategický cíl 3 Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu, specifický cíl 3. 2 - Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů ICT a hlavní aktivita č: 7. Zvýšení kybernetické bezpečnosti IKT VS čili projektový okruh Kybernetická bezpečnost, jehož garantem je NBÚ. Jeho indikátorem jsou Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti. Projekt reaguje na zvyšující se potřebu řešení kybernetické bezpečnosti a váže se na realizaci jediného specifického cíle, kterým je **dobudování informačních a komunikačních systémů veřejné správy a realizace bezpečnostních opatření podle zákona o kybernetické bezpečnosti**. Projekt je popsán v kapitole číslo 5.4, ale obecně informační systémy veřejné správy (ISVS) mají z hlediska kybernetické bezpečnosti různou úroveň zabezpečení. Skutečně důležité systémy ISVS jsou určovány Národním bezpečnostním úřadem jako prvky Kritické informační infrastruktury (KIT) nebo Významné informační systémy (VIS). Pro chod státu a společnosti je nezbytné jejich bezchybné fungování v podobě zajištění důvěrnosti, integrity a dostupnosti jejich dat. Cílem projektu je zajistit průběžný monitoring a vyhodnocování kybernetických hrozeb ve vybraných informačních systémech veřejné správy (ISVS). Prostředky k dosažení cíle: fyzické rozmístění prvků sledování síťového provozu ve vybraných systémech ISVS, jejich propojení a následné spuštění systému monitorování kybernetických událostí včetně softwarového vybavení a potřebných výpočetních a

úložných kapacit včetně zálohování.

5.3. Návaznost projektu na další aktivity žadatele

V průběhu přípravné fáze projektu byla obecně analyzována ICT bezpečnost úřadu. Byla brána v potaz i aktualizovaná analýza rizik.

Projekt významně zvyšuje úroveň zabezpečení stávajících systémů úřadu. Navazuje na předchozí projekt žadatele z výzvy č. 08 Integrovaného operačního programu "**Technologické centrum Pardubického kraje"** a na projekt z výzvy č. 19 „**Bezpečnostní infrastruktura technologického centra Pardubického kraje**". Technická opatření navržená v rámci řešení doplňují nebo rozšiřují funkcionalitu stávajících ICT systémů tak, aby naplňovala požadavky definované zákonem. Dodávky v rámci projektu neduplikují stávající řešení.

5.4. Podrobný popis jednotlivých aktivit projektu

5.4.1. Popis realizace hlavních aktivit projektu ve smyslu kap. 2.2 Specifických pravidel

Hlavní podporovanou aktivitou je zabezpečení KII/VIS/ISZS/IS/KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014. Sb., o kybernetické bezpečnosti, ve znění pozdějších a doprovodných předpisů.

Hlavními podporovanými aktivitami jsou následující technická opatření:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti KII a VIS, jejich uživatelů a administrátorů,
- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací,
- bezpečnost průmyslových a řídicích systémů.

Tato opatření budou mimo fyzickou bezpečnost realizována všechna a jejich návaznost je popsána v kapitole 10.

Následující hlavní aktivity uvádíme pro přehlednost i s číslem paragrafu vyhlášky 316/2104 Sb.:

5.4.1.1. §16 - Fyzická bezpečnost

Toto opatření nebylo v rámci projektu řešeno.

5.4.1.2. §17 - Nástroj pro ochranu integrity komunikačních sítí

V rámci projektu „Bezpečnost komunikační infrastruktury" je tento paragraf řešen postupnou implementací opatření č. 2 - Implementace VPN brány, opatření č. 4 – Doplnění přístupových přepínačů a opatření č. 10 – Doplnění redundantní [redacted] proxy. Detailní informace o těchto opatřeních jsou popsány v kapitolách 8.1.3, 8.1.5 a 8.1.11

5.4.1.3. §18 - Nástroj pro ověřování identity uživatelů

Projekt řeší tento paragraf nasazením pěti opatření, a to konkrétně opatřením č. 1 - Implementace správy

privilegovaných uživatelů a účtů, opatřením č. 2 - Implementace VPN brány, opatřením č. 4 - Doplnění přístupových přepínačů, opatřením č. 6 – Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě a opatření č. 15 – Více faktorové ověřování identity uživatelů a administrátorů informačních systémů. Veškeré detaily k tomu lze dohledat v kapitolách 8.1.2, 8.1.3, 8.1.5, 8.1.7 a 8.1.16.

5.4.1.4. §19 - Nástroj pro řízení přístupových oprávnění

Požadavky dané paragrafem 19 jsou naplněny implementací opatření č. 4 – Doplnění přístupových přepínačů a opatření č. 6 – Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě, které jsou popsány v kapitolách 8.1.5 a 8.1.7.

5.4.1.5. §20 - Nástroj pro ochranu před škodlivým kódem

V projektu je §20 naplněn pomocí opatření č. 9 - Implementace řešení pro monitorování toků a opatření č. 11 – Rozšíření [redacted] o SANDBOX. Jejich detailní vysvětlení naleznete v kapitolách 8.1.10 a 8.1.12 tohoto dokumentu.

5.4.1.6. §21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

Projektem je tento paragraf řešen pomocí zavedení opatření č. 1 - Implementace správy privilegovaných uživatelů a účtů, nasazením opatření č. 7 – Centrální logovací nástroj a opatřením č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS. Veškeré detaily o vybraných řešeních a jejich popis naleznete v kapitolách 8.1.2, 8.1.8 a 8.1.14.

5.4.1.7. §22 - Nástroj pro detekci kybernetických bezpečnostních událostí

Projekt řeší tento paragraf nasazením pěti opatření č. 4 – Doplnění přístupových přepínačů, opatření č. 9 - Implementace řešení pro monitorování toků a opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru, která jsou podrobně popsána v kapitolách 8.1.5,8.1.10 a 8.1.13.

5.4.1.8. §23 - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Toto opatření nebylo v rámci projektu řešeno.

5.4.1.9. §24 - Aplikační bezpečnost

V projektu je paragraf 24 aplikační bezpečnost naplňován nasazením opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru, opatření č. 17 - Implementace testovacího centra a opatření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management. Tato opatření a jejich konkrétní volby jsou podrobně popisovány v kapitolách 8.1.13, 8.1.18 a 8.1.19.

5.4.1.10. §25 - Kryptografické prostředky

Aby úřad naplnil požadavky paragrafu 25 jsou v projektu „Bezpečnost komunikační infrastruktury“ zahrnuta opatření č. 2 - Implementace VPN brány, opatření č. 4 – Doplnění přístupových přepínačů a opatření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů. Jejich detailní popisy naleznete v kapitolách 8.1.3, 8.1.5 a 8.1.15.

5.4.1.11. §26 - Nástroj pro zajišťování úrovně dostupnosti

Vzhledem k tomu, že si zaměstnanci IT oddělení úřadu uvědomují důležitost dostupnosti jednotlivých informačních systémů je toto na úrovni podpůrných prostředků naplňováno pomocí sedmi opatření, která jsou zmíněna dále, a to konkrétně opatřením č. 3 - Zajištění redundance optických tras pro přístupové switche, opatřením č. 4 – Doplnění přístupových přepínačů, opatřením č. 5 - Doplnění HW Datového centra o servery a pole, opatřením č. 8 - Implementace vysoké dostupnosti pro [redacted] opatřením č. 10 – Doplnění redundantní [redacted] proxy, opatřením č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru a opatřením č. 16 – Rozšíření stávajícího dohledového centra [redacted] Veškerá tato opatření jsou detailně popisována v kapitolách 8.1.4, 8.1.5, 8.1.6, 8.1.9, 8.1.11, 8.1.13 a 8.1.17 tohoto dokumentu.

5.4.1.12. §27 - Bezpečnost průmyslových a řídicích systémů

Toto opatření nebylo v rámci projektu řešeno.

Pro zpřehlednění níže uvádíme tabulku ukazující vazby mezi jednotlivými paragrafy a opatřeními implementovanými v rámci projektu „Bezpečnost komunikační infrastruktury“.

	Opatření č. 1 - Implementace správy privilegovaných uživatelů a účtů	Opatření č. 2 - Implementace VPN brány	Opatření č. 3 - Zajištění redundance optických tras pro přístupové switche	Opatření č. 4 – Doplnění přístupových přepínačů	Opatření č. 5 - Doplnění HW Datového centra o servery a pole	Opatření č. 6 – Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě	Opatření č. 7 – Centrální logovací nástroj	Opatření č. 8 - Implementace vysoké dostupnosti pro [redacted]	Opatření č. 9 - Implementace řešení pro monitorování toků	Opatření č. 10 – Doplnění redundantní [redacted] proxy	Opatření č. 11 – Rozšíření [redacted] o SANDBOX	Opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru	Opatření č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS	Opatření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů	Opatření č. 15 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů	Opatření č. 16 – Rozšíření stávajícího dohledového centra [redacted]	Opatření č. 17 - Implementace testovacího centra	Opatření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management
§15 - Kontrola a audit kybernetické bezpečnosti																		
§16 - Fyzická bezpečnost	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
§17 - Nástroj pro ochranu integrity komunikačních sítí		X		X						X								
§18 - Nástroj pro ověřování identity uživatelů	X	X		X		X									X			
§19 - Nástroj pro řízení přístupových oprávnění				X		X												
§20 - Nástroj pro ochranu před škodlivým kódem									X		X							
§21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů	X						X						X					

§22 - Nástroj pro detekci kybernetických bezpečnostních událostí				X					X			X						
§23 - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
§24 - Aplikační bezpečnost												X					X	X
§25 - Kryptografické prostředky		X		X										X				
§26 - Nástroj pro zajišťování úrovně dostupnosti			X	X	X			X		X		X				X		
§27 - Bezpečnost průmyslových a řídicích systémů	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Tabulka 5 - Přehled hlavních aktivit – vazby s navrženými opatřeními

5.4.2. Popis realizace vedlejších aktivit projektu ve smyslu kap. 2.2 Specifických pravidel (např. zpracování projektové dokumentace)

V kap. 2.2 Specif.pravidel jsou vedlejšími podprovanými aktivitami:

- pořízení studie proveditelnosti,
- zpracování zadávacích podmínek k zakázkám a na organizaci výběrových a zadávacích řízení,
- odborné konzultace a dozor při implementaci,
- bezpečnostní audit a penetrační testy,
- cloudová řešení (do doby ukončení realizace projektu),
- projektová dokumentace stavebních prací a úprav,
- technický dozor investora, BOZP, autorský dozor
- povinná publicita.

Žadatel bude realizovat:

- pořízení této Studie proveditelnosti jako nezpůsobilý výdaj
- zpracování zadávacích podmínek k zakázkám a na organizaci výběrových a zadávacích řízení,
- odborné konzultace a dozor při implementaci,
- bezpečnostní audit a penetrační testy,
- povinnou publicitu.

Podrobný popis těchto aktivit je uveden v následujících podkapitolách.

5.4.2.1. Studie proveditelnosti

Je již zpracována a bude doložena jako povinná příloha k žádosti o podporu.

5.4.2.2. Zpracování zadávacích podmínek k zakázkám a na organizaci výběrových a zadávacích řízení

VŘ na právní služby spojené s vypsáním výběrového řízení na projekt

úřad připraví a vypíše výběrové řízení na dodavatele právních služeb spojených s vypsáním veřejné zakázky na implementaci projektu bezpečnosti, vybere vítěze a uzavře s ním řádnou smlouvu.

VŘ na implementaci bezpečnostního projektu

úřad spolu s vybraným dodavatelem právních služeb připraví detailní specifikace a veškeré formality nutné

k vypsání výběrového řízení na kompletní projekt dodávky HW, SW, implementační práce a ostatní služby s projektem spojení včetně následné podpory zajistí jeho zveřejnění. V rámci kontinuity je projekt uvažován jako celek obsahující všechny dílčí části. Vyhodnocení a objednání projektu. Výběrová komise spolu se zodpovědnými pracovníky krajského úřadu provedou vyhodnocení výběrového řízení a provede vyhlášení vítěze.

5.4.2.3. Odborné konzultace a dozor při implementaci

Žadatel vysoutěží externí/ho dodavatele, který bude v průběhu implementace bezpečnostního projektu poskytovat odborné konzultace a dozor nad implementací projektu.

5.4.2.4. Bezpečnostní audit a penetrační testy

Provedení GAP analýzy je bezpečnostním auditem projektu a je formálně rozděleno do tří po sobě jsoucích fází, kdy v první z nich proběhne rekognoskace prostředí krajského úřadu, jejímž cílem je získání potřebných informací pro zpracování GAP analýzy. Ve druhé fázi jsou získaná data porovnávána z požadavky ZKB a Dodavatel identifikuje a hodnotí zjištěné rozdíly, které zaznamená do rozdílové zprávy. Následně ve třetí fázi Dodavatel spolu se odpovědnými pracovníky krajského úřadu navrhuje nápravná opatření.
Realizace této aktivity se předpokládá v období 9/2017–11/2017

5.4.2.5. Povinná publicita

Žadatel zrealizuje dle Obecných pravidel pro žadatele a příjemce nákup informačních tabulí, pamětních desek..

5.4.3. Zaškolení technologií a postupů

- Součástí implementací každého opatření budou i nutná zaškolení správců sítě Pardubického kraje. Některá opatření jsou technologicky nová, jiná významně rozšiřují stávající odborné znalosti administrátorů. Jednotlivá zaškolení tak budou ve fázích:
    - Před vlastní implementací opatření – seznámení s technologií, důležité pojmy, procesy
    - Instalace, implementace opatření za přítomnosti pracovníků oddělení informatiky
    - Zaškolení provozu, bezpečnosti a administrace opatření po jeho implementaci
- Na závěr bude následovat školení pro administrátory sítě, pojímající všechna implementovaná i stávající opatření jako celek.

5.4.4. Popis ukončení realizace projektu

Ukončení realizace projektu bude provedeno těmito kroky:

- Akceptace díla
- Předání celku do testovacího provozu
- Vyhodnocení testovacího provozu
- Úpravy dle výsledků testovacího provozu
- Finální akceptace celého projektu

- Zaškolení zaměstnanců úřadu
- Předání do užívání KrÚ PK

Ukončení realizace projektu předpokládáme ke dni 22.11.2019.

5.5. Časový harmonogram realizace podle etap

5.5.1. Časová období, zvýraznění počátku a konce etapy, jejich náplň a návaznost

Projekt bude jednoetapový. Nicméně je rozdělen do dvou následujících fází, které jsou dle potřeby následně členěny do dílčích implementačních částí. Začátek etapy bude okamžikem schválení proketu Radou kraje a konec etapy na 22.11.2019. Náplň etapy je popsána v jednotlivých implementačních částech níže v podkapitolách. Bude zakončeno standardním ukončovacím procesem předání díla a akceptace včetně testovacího provozu. Po fakturaci dodavatelem bude zpracována Závěrečná monitorovací zpráva a vystavena zjednodušená Žádost o platbu do 20 kalendářních dnů po konci etapy.

Přípravná fáze 1.6.2016 – 31.10.2017

V rámci této fáze proběhnou všechny nutné kroky nutné pro řádnou přípravu implementace

- **Výběr varianty řešení, vypracování příslušné Studie proveditelnosti** – v této části žadatel spolu se security odborníky smluvního dodavatele provede důkladné posouzení jednotlivých řešení z hlediska technické náročnosti a nákladů na jeho realizaci. Provede definici bezpečnostních prvků a opatření a navrhl postup implementace.
- **Zpracování žádosti o dotaci** – nedílnou součástí přípravné fáze bylo zpracování žádosti do IROP včetně všech povinných příloh.
- **Zajištění financování** – na základě výstupů z výběru žadatel zajistí v rámci úřadu dostatečné prostředky pro financování výdajů spojených s realizací Projektu a to jak investičního, tak neinvestičního charakteru.
- **Schválení žádosti o dotaci Radou** – výsledné podklady včetně finančních kalkulací budou předloženy krajské radě a proběhne jejich schválení.

VŘ na právní služby spojené s vypsáním výběrového řízení na projekt

- úřad připraví a vypíše výběrové řízení na dodavatele právních služeb spojených s vypsáním veřejné zakázky na implementaci projektu bezpečnosti, vybere vítěze a uzavře s ním řádnou smlouvu.

VŘ na implementaci bezpečnostního projektu

- úřad spolu s vybraným dodavatelem právních služeb připraví detailní specifikace a veškeré formality nutné k vypsání výběrového řízení na kompletní projekt dodávky HW, SW, implementační práce a ostatní služby s projektem spojení včetně následné podpory zajistí jeho zveřejnění. V rámci kontinuity je projekt uvažován jako celek obsahující všechny dílčí části.

Vyhodnocení a objednání projektu

- výběrová komise spolu se zodpovědnými pracovníky krajského úřadu provedou vyhodnocení výběrového řízení a provede vyhlášení vítěze.

Sestavení projektového týmu

Žadatel po uzavření smlouvy s dodavatelem, který následně vytvoří externí projektový tým ve složení v kapitole 7. Bude vytvořena komunikační matice, specifikovány úkoly a odpovědnosti jednotlivých členů týmu, specifikován detailní harmonogram a zahájena realizace projektu.

5.5.1.1. Implementační část č. 1 - Provedení GAP analýzy

- Provedení GAP analýzy je formálně rozděleno do tří po sobě jsoucích fází, kdy v první z nich proběhne rekognoskace prostředí krajského úřadu, jejímž cílem je získání potřebných informací pro zpracování GAP analýzy. Ve druhé fázi jsou získaná data porovnávána z požadavky ZKB a Dodavatel identifikuje a hodnotí zjištěné rozdíly, které zaznamená do rozdílové zprávy. Následně ve třetí fázi Dodavatel spolu se odpovědnými pracovníky krajského úřadu navrhuje nápravná opatření.
- Realizace této aktivity se předpokládá v období 9/2018 – 10/2018

5.5.1.2. Implementační část č. 2 – Implementace správy privilegovaných uživatelů a účtů

- Před samotnou implementací je nutné potvrdit cílovou architekturu v rámci předimplementační analýzy, která zodpoví detailně všechny technické aspekty budoucího nasazení, včetně rozhodnutí, jaké skupiny privilegovaných účtu a uživatelů budou součástí řešení, u kterých se bude provádět sledování celého životního cyklu privilegovaného účtu (vytváření, přidělování přístupu, změny hesel atd.) Následují technické instalace a konfigurace všech komponent, a import všech dotčených účtů. V rámci přechodu na nový způsob nakládání s privilegovanými účty a díky dopadům na fungování jak interních zaměstnanců, tak externích dodavatelů je nutné připravit uživatelské příručky, případně provést školení jednotlivých skupin uživatelů. Zároveň je nutné upravit proces správy privilegovaných účtů v rámci organizace. Následuje pilotní a testovací provoz na vybrané skupině uživatelů, úpravy konfigurací a nasazení do ostrého provozu.
- Realizace této aktivity se předpokládá v období 08/2018 – 10/2018

5.5.1.3. Implementační část č. 3 - Implementace VPN brány

- V rámci implementace VPN brány bude převedena konfigurace ze stávajícího řešení na nové. Základní část konfigurace bude beze změny. Zásadní změnou bude použití silnějších algoritmů pro sestavované šifrované VPN tunely. U „LAN to LAN“ IPSec VPN se použije IKE protokol verze 2 a zároveň šifrovací algoritmy ze SUITE B standartu. Pro mobilní uživatele dojde k upgradu koncových VPN klientů na aktuální verzi. Zde se nejdříve provede test kompatibility s ostatním softwarovým vybavením používaným na počítačích kraje.

  Dále po implementaci nástroje bude provedena integrace s centrálním logovacím systémem pro zaznamenání případných informací, na jejichž základě se zjistí případné KBU a KBI.

- Realizace této aktivity se předpokládá v období 08/2018 – 10/2018

5.5.1.4. Implementační část č. 4 - Zajištění redundance optických tras pro přístupové switche

- Jako výchozí krok instalace optických kabelových tras bude proveden průzkum lokality, zaměření tras, návrh prostupů. Následně po odsouhlasení dojde k nutným stavebním pracem a instalace drátěných kabelových žlabů, multiduct kanálu do drátěných tras a instalace mikrotrubiček včetně odboček z multiduct kanálu. Paralelně bude provedena instalace HDPE trubek do kolektoru a protažení mikrotrubiček HDPE trasou. Ve finální fázi dojde k zafouknutí optických mikrokabelů. V rozvaděčích budou instalovány optické vany a zavařeny pigtaily na optická vlákna. Před předáním díla dojde k instalaci požárních ucpávek do průrazů mezi požárními úseky a bude provedeno měření FO kabelů útlumovou metodou. Součástí dodávky bude dokumentace skutečného provedení.
- Realizace této aktivity se předpokládá v období 08/2018 – 10/2018

5.5.1.5. Implementační část č. 5 – Doplnění přístupových přepínačů

- V rámci implementace doplnění LAN přepínačů dojde k obměně zařízení, které jsou zastaralá a jsou mimo podporu výrobce. U těchto zařízení dojde k jejich fyzické instalaci. Použije se stávající konfigurace a doplní se o nová bezpečnostní nastavení (802.1x, ARP inspekce atd.), která nové modely přepínačů podporují a jsou v souladu se stávajícím designem LAN.
- Dále se doplní dvojice páteřních přepínačů o 10 Gbps servisní kartu, která umožní zbudování redundantních datových cest mezi přístupovými a páteřními přepínači. Zde se upraví konfigurace v páteřních přepínačích a zároveň se rozšíří nastavení v přístupových přepínačích.
- Pro datový propoj mezi páteřní sítí a spisovnou se vytvoří zcela nová konfigurace. A to s nastavením MAC SEC šifrování na pronajmuté optické trase.
- Z pohledu detekce KBU se upraví nastavení všech přepínačů o zasílání dat pomocí NetFlow protokolu na centrální kolektor. Dále se provede integrace s centrálním logovacím nástrojem pro zaznamenání případných informací, na jejichž základě se zjistí případné KBU a KBI.
- Realizace této aktivity se předpokládá v období 10/2018

5.5.1.6. Implementační část č. 6 - Doplnění HW Datového centra o servery a pole

- V rámci implementace prostředků datového centra dojde k vybudováníinfrastruktury ve dvou lokalitách, která bude připojená ke stávajícímu prostředí. Toto prostředí bude sloužit pro běh aplikací a ukládání dat vyplývajících z ostatních opatření.
- V každé lokalitě bude vybudována nová LAN infrastruktura skládající se ze dvou páteřních přepínačů na lokalitu. Páteřní přepínače jsou propojeny jak v rámci lokality, tak mezi lokalitami a zjišťují centrální přepínací systém pro ethernet provoz v rámci lokality i mezi lokalitami.
- Výpočetní výkon zajišťují rackové servery. Část serverů je virtualizována pomocí [redacted] a část bude bare metal s přímou instalací operačního systému na fyzický server.
- Pro komunikaci na diskový systém bude využívána oddělená SAN infrastruktura. Pro tento účel se plánuje využít stávající SAN přepínače společnosti [redacted]

- Pro ukládání dat bude implementován diskový systém v konfiguraci stretched metrocluster. Diskový systém bude virtualizován, tak aby došlo ke kompletnímu oddělení dle typu aplikace nejen na úrovni diskového prostoru, ale také na úrovni správy.
- Realizace této aktivity se předpokládá v období 11/2018 – 12/2018

5.5.1.7. Implementační část č. 7 - Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě

- V rámci implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě bude nejdříve provedena analýza požadavků, stávající infrastruktury a IT procesů. Následně dojde k aktualizaci systémových komponent, navrženo a implementováno řešení.
- Aplikace pro administraci a obsluhu 802.1x budou nainstalovány. Bude provedeno nastavení základních síťových a aplikačních parametrů a nastavena komunikace s přepínači pomocí SNMP a SSH. Po odzkoušení komunikace mezi Cisco ISE – aplikacemi 802.1x – LDAP, bude provedeno zaškolení uživatelů a aplikace předány k užívání.
- Realizace této aktivity se předpokládá v období 01/2019 – 4/2019

5.5.1.8. Implementační část č. 8 – Centrální logovací nástroj

- Před samotnou implementací je nutné provést implementační analýzu, která definuje zdrojové systémy, zhodnotí jejich aktuální kvalitu auditní stopy a případně doporučí změny v nastavení auditní politiky na zdrojových systémech. Zároveň definuje pro každý typ zdrojového systému, jaká bude metoda sběru logů s ohledem na jeho technické možnosti a architekturu řešení. Následuje technická fáze připojení zdrojových systémů, a konfigurace centrální konzole (vyhledávání, dashboardy, reporty, alerty). Následuje zaškolení administrátorů řešení a přizpůsobení centrální konzole pro jednotlivé typy uživatelů (admin, IT manager, auditor, atd.)
- Realizace této aktivity se předpokládá v období 01/2019 – 2/2019

5.5.1.9. Implementační část č. 9 - Implementace vysoké dostupnosti pro [redacted]

- V rámci implementace vysoké dostupnosti pro [redacted] se provede instalace replikačních scriptů, které provedou zálohu [redacted] databáze na záložní server. V případě výpadku se provede přesměrování dotazů ze strany klientů VIS na tuto záložní databázi. Výsledkem je značné zkrácení výpadku VIS na akceptovatelnou úroveň.
- Realizace této aktivity se předpokládá v období 01/2019

5.5.1.10. Implementační část č. 10 – Implementace nástroje pro monitorování toků

- V rámci implementace se provede fyzická instalace kolektoru do racku a základní nastavení-zejména nastavení IP adresy kolektoru na kterou se budou zasílat exportovaná netflow data z centrálních přepínačů. Na centrálních přepínačích se nakonfiguruje netflow monitor pro sledování dat na L3 rozhranních a netflow exporter pro zasílání dat na netflow kolektor. Další částí implementace bude zprovoznění netflow kolektoru, kdy se provede validace přijímaných dat a nastavení úložné kapacity

pro nasbíraná data. Nakonec se nakonfigurují filtry pro behaviorální analýzu, aby se zamezilo výskytu „false positive“ událostí.

- Realizace této aktivity se předpokládá v období 01/2019

5.5.1.11. Implementační část č. 11 – Doplnění redundantní [redacted] proxy

- V rámci implementace nové [redacted] proxy bude převedena konfigurace ze stávajícího řešení na nové. Dojde k upgradu a nastavení operačního systému [redacted] proxy dle prostředí zákazníka. Dále se provede integrace s centrálním logovacím nástrojem pro zaznamenání případných informací, na jejichž základě se zjistí případné KBU a KBI.
- Realizace této aktivity se předpokládá v období 01/2019

5.5.1.12. Implementační část č. 12 – Rozšíření [redacted] o SANDBOX

- V rámci implementace SandBoxingu pro webový provoz bude nasazena dvojice sandboxovacích zařízení. Tyto zařízení budou komunikovat se stávajícími proxy branami. Proxy brány budou předávat podezřelé soubory k analýze do sandboxu, kdy dojde k jejich prověření. Vytvoří se kopie operačních systémů, které budou odpovídat reálnému prostředí. Tím se výsledná analýza chování potencionální škodlivého kódu co nejvíce přiblíží reálnému prostředí. Dále se provede integrace s centrálním logovacím nástrojem pro zaznamenání informací, na jejichž základě se zjistí případné KBU a KBI.
- Realizace této aktivity se předpokládá v období 01/2019 – 2/2019

5.5.1.13. Implementační část č. 13 – Implementace Webového aplikačního firewallu a Loadbalanceru

- Implementace WAF spolu s ochranou před DDoS útoky je členěna do dvou kroků:
  - Implementace WAF bude probíhat v třech fázích. Po identifikaci základních politik pro vytvoření filtrovacích pravidel firewall (ACL) budou dale identifikovány objekty pro ochranu před DoS útoky.
  - Každá chráněná aplikace bude disponovat vlastní nezávislou politikou, aby bylo možné vytvořit granulární a specifickou politiku pro každou aplikaci, či aplikační platformu/framework.
  - Politika WAF pro každou aplikaci bude obsahovat signatury schopné zachytit známé aplikační útoky a měla by obsahovat specifické nastavení pro každou aplikaci (ochrana cookies, URL, parametrů apod.).
  - Součástí nastavení WAF bude také ochrana proti L7 DoS útokům prostředky dostupnými ve WAF. V aplikacích, které vyžadují přihlášení uživatele by bezpečností politika obsahovala také Brute Force ochranu.
  - V případě aplikace využívající HTTPS protokol je nutné, aby SSL spojení bylo na WAF terminováno.
- Realizace této aktivity se předpokládá v období 02/2019 – 4/2019

5.5.1.14. Implementační část č. 14 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS

- V rámci implementace modulu „transakčního logu“ dojde k rozšíření logovacích schopností administrační části GINIS systému a i vytváření transakčního logu k jednotlivým modulům systému. Zalogované informace z jednotlivých modulů budou exportovány do PDF, a to s digitálním podpisem a časovým razítkem. Dalším krokem bude nastavení zabezpečeného přenosu infromací mezi GINIS aplikací a datovým uložištěm. V neposlední řadě se provede integrace s centrálním logovacím nástrojem pro zaznamenání případných informací, na jejichž základě se zjistí případné KBU a KBI.
- Realizace této aktivity se předpokládá v období 01/2019

5.5.1.15. Implementační část č. 15 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů

- Implementace proběhne současně s etapou č. 15 a v jejím průběhu bude konektor nejprve zprovozněn na testovacím systému a ověřena jeho funkčnost s datovým úložištěm a následně bude nainstalován do živého prostředí a přenesena ověřená konfigurace.
- Realizace této aktivity se předpokládá v období 01/2019 – 2/2019

5.5.1.16. Implementační část č. 16 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů

- Implementace dvoufaktorového ověřování je navázána na zajištění procesní správnosti a je tvořena jednak dopněním HW tam, kde je to vyžadováno a za druhé instalací obslužného SW do koncových stanic, kde bude využívána. Z pohledu administrace jde o standardní úkon, který lze provést buď lokálně, nebo dávkově prostřednictvím centrální správy a služeb MS Active Directory. Následně je třeba zajistit vydávání čipových karet včetně distribuce certifikátů a jejich centrální správy.
- Realizace této aktivity se předpokládá v období 4/2019 – 5/2019

5.5.1.17. Implementační část č. 17 – Rozšíření stávajícího dohledového centra [redacted]

- Implementace systému [redacted] spočívá v jeho přenesení na nový. Nejprve bude provedeno odstavení stávající instance systému a provedena záloha, aby bylo možné zachovat jmennou a adresní konvenci stávajícího řešení. Následně bude provedena instalace OS a nové SW instance [redacted]. Do této se pak zmigruje původní konfigurace. Následně se systém nastartuje a ověří se správnost funkcionality.
- Realizace této aktivity se předpokládá v období 02/2019

5.5.1.18. Implementační část č. 18 – Implementace testovacího centra

- Implementace systému je velmi jednoduchá – jedná se o aplikaci, kterou je možné standardním způsobem nainstalovat na většinu systémů s OS Windows.
- Realizace této aktivity se předpokládá v období 02/2019–3/2019

5.5.1.19. Implementační část č. 19 – Implementace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management

- Implementace systému je relativně přímočará – instalace centrální konzole i skeneru může být provedena na jediném počítači s OS Windows nebo Linux, případně formou virtuálního zařízení. Doplňkově je možné další skener (případně oba) instalovat na jiném stroji s uvedenými OS. Jediným doplňkovým požadavkem je v tomto případě zajištění prostupů na komunikační porty, pomocí nichž centrální konzole a skenery komunikují, v ACL v relevantních systémech a síťových prvcích.
    - Realizace této aktivity se předpokládá v období 02/2019

5.5.2. Popis realizace vedlejších aktivit projektu

Veškeré vedlejší aktivity projektu budou realizovány v souladu s platnou legislativou a s pravidly pro žadatele a příjemce platnými pro průběžnou výzvu č. 10. Do těchto aktivit projektu budou zahrnuty náklady na přípravné činnosti. Mimo jiné:

- náklady na právní služby spojené s vypracováním kompletní zadávací dokumentace k veřejné zakázce a na organizaci výběrových a zadávacích řízení,
- náklady na odborné konzultace a dozor při implementaci projektu
- náklady na zajištění potřebné publicity projektu,
- audit a bezpečnostní analýza, tzn. GAP analýzu a penetrační testy

Provedení GAP analýzy

Činnosti spojené s provedením GAP analýzy jsou popsány v kapitole 5.6 ve článku Implementační část č. 1 - Provedení GAP analýzy.

- V první fázi proběhne rekognoskace prostředí krajského úřadu, jejímž cílem je získání potřebných informací pro zpracování GAP analýzy. V této fázi probíhá intenzivní spolupráce odpovědných zaměstnanců krajského úřadu s Dodavatelem.
- Ve druhé fázi jsou vytěžená data porovnávána z požadavky ZKB a Dodavatel identifikuje a hodnotí zjištěné rozdíly.
- Ve třetí fázi Dodavatel spolu se odpovědnými pracovníky krajského úřadu navrhuje nápravná opatření a upravuje konfiguraci dodávaných opatření v souladu se změnami.

Ukončovací fáze

- **Penetrační testy** – Po ukončení implementace a kompletním odladění všech dílčích systémů bude v průběhu zkušebního provozu před zahájením ostrého provozu proveden nezávislý penetrační test a bude provedeno jeho vyhodnocení. Na základě jeho výsledku proběhnou případné úpravy jednotlivých funkcionalit, nebo procesů a zahájen plný provoz.
- **Administrace Projektu** – monitoring projektu a reporting v souladu s požadavky poskytovatele dotace bude zajišťovat žadatel.
- **Audit Projektu** – nedílnou součástí investiční fáze je povinný audit dle pravidel programu. Audit projektu.

Provozní fáze – fáze udržitelnosti

- **Provozování nové technologie –** pořízený SW/HW bude využíván pro poskytování služeb žadatele po celou dobu udržitelnosti projektu.
- **Publicita Projektu –** v rámci provozní etapy bude zajištěna publicita dle pravidel IROP.
- **Monitoring a reporting Projektu** – v souladu s požadavky poskytovatele dotace bude zajišťovat žadatel.

5.5.3. Časový harmonogram projektu

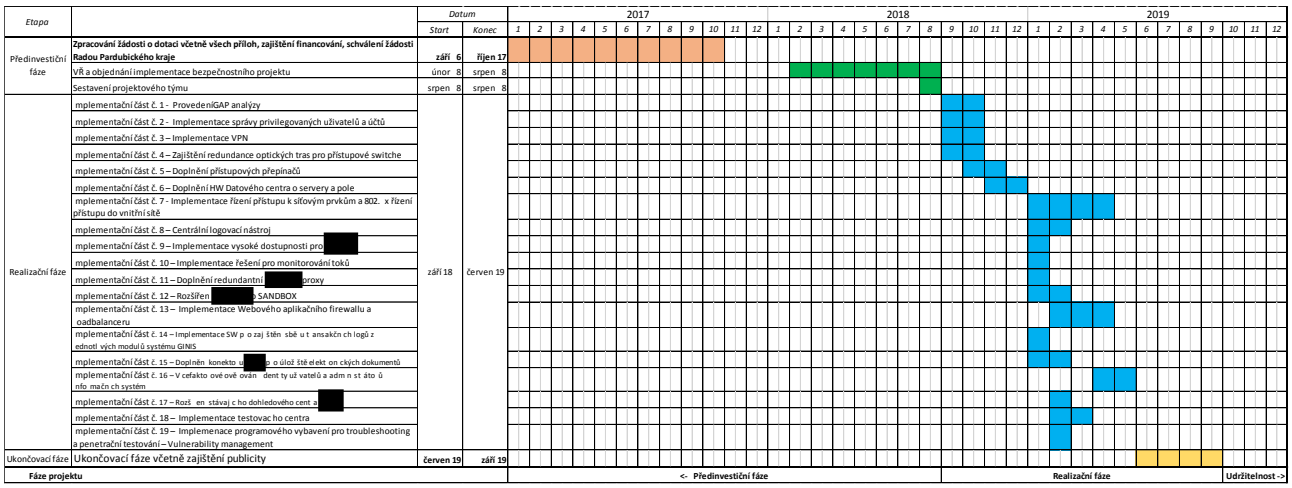
Na základě zkušeností s implementací obdobných projektů s přihlédnutím na kapacitní možnosti zaměstnanců KÚ Pardubického kraje byl ve spolupráci s odbornými pracovníky dodavatelů navržen časový harmonogram projektu.

Projekt je rozdělen na fáze přípravné, realizační a fázi udržitelnosti. Zároveň je členěn do jednotlivých implementačních částí pokrývajících všechna navržená opatření.

Etapa	*Popis činnosti*	*Datum*	
		Start	*Konec*
	Předinvestiční fáze	**Září 2016**	**Říjen 2017**
	VŘ a objednání implementace bezpečnostního projektu	**Únor 2018**	**Srpen 2018**
	Sestavení projektového týmu	Srpen 2018	Srpen 2018
	Implementační část		
1	Implementační část č. 1 - ProvedeníGAP analýzy		
2	Implementační část č. 2 - Implementace správy privilegovaných uživatelů a účtů		
3	Implementační část č. 3 – Implementace VPN		
4	Implementační část č. 4 – Zajištění redundance optických tras pro přístupové switche		
5	Implementační část č. 5 – Doplnění přístupových přepínačů		
6	Implementační část č. 6 – Doplnění HW Datového centra o servery a pole		
7	Implementační část č. 7 - Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě		
8	Implementační část č. 8 – Centrální logovací nástroj		
9	Implementační část č. 9 – Implementace vysoké dostupnosti pro [redacted]		
10	Implementační část č. 10 – Implementace řešení pro monitorování toků	**Září 2017**	**Květen 2019**
11	Implementační část č. 11 – Doplnění redundantní [redacted] proxy		
12	Implementační část č. 12 – Rozšíření [redacted] o SANDBOX		
13	Implementační část č. 13 – Implementace Webového aplikačního firewallu a Loadbalanceru		
14	Implementační část č. 14 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS		
15	Implementační část č. 15 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů		
16	Implementační část č. 16 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systém		
17	Implementační část č. 17 – Rozšíření stávajícího dohledového centra [redacted]		
18	Implementační část č. 18 – Implementace testovacího centra		
19	Implementační část č. 19 – Implemenace programového vybavení pro troubleshooting a penetrační testování – Vulnerability management		

	Ukončovací fáze včetně zajištění publicity	Červen 2019	Září 2019

Tabulka 6 Stručný časový harmonogram projektu



Tabulka 7 Grafické znázornění časového harmonogramu projektu

5.5.4. Termíny zahájení a ukončení realizace projektu.

Termíny zahájení a ukončení realizace projektu jsou patrné z Tabulky 6 Časový harmonogram projektu.

5.6. Identifikace negativních dopadů projektu

5.6.1. Výčet všech negativních dopadů realizace a provozu projektu, jejich popis a předpokládaní nositelé

- Jedinými minoritními identifikovanými dopady je zvýšení nároků kladených na obsluhu navržených technických opatření vedoucí požadavku na lidské zdroje zadavatele (jejich pravidelné školení) a nevýznamné zvýšení provozních nákladů (elektrické energie a chlazení)
- V rámci přípravy projektu nebyly identifikovány další zásadní negativní dopady.
- Nositelem negativních dopadů je tedy energetická a časová náročnost realizace a provozu projektu

5.6.2. Návrhy na eliminaci negativních dopadů

- Navýšení rozpočtu kraje na provozní náklady
- Zvážit navýšení kapacit lidských zdrojů s potřebnou kvalifikací.
- Zvážit navýšení zdrojů na udržení a povýšení kvalifikace lidských zdrojů.

5.7. Popis investiční a nulové varianty

Byly zvažovány následující varianty řešení:

Nulová varianta – předpokládá zachování stávajícího stavu a bude zachována stávající míra bezpečnosti krajského úřadu, a to jak vnitřní, tak i vnější. Tato varianta neumožňuje takovou míru bezpečnosti, jaká je vyžadována platnou legislativou.

Výhody

- nulová investice a provozní náklady (úspora materiálových, finančních, lidských zdrojů),
- odpadá riziko, že dotace nebude přidělena,
- Pardubický kraj se nezavazuje k udržení výstupů projektu.

Nevýhody

- nevybudování potřebných technických opatření, jež je povinen Pardubický kraj realizovat na základě požadavků Zákona o kybernetické bezpečnosti a běžných standardů kybernetické bezpečnosti pro eliminaci či ponížení rizik plynoucí z běžného provozu počítačové sítě významného Orgánu veřejné moci.

Investiční varianta - rozšíření stávajících systémů tak, aby jednak poskytovaly požadavky na danou funkcionalitu v rámci nutných podmínek stanovených příslušnou legislativou, dále aby rozšíření stávajících systémů bylo i v souladu s Informační strategií Pardubického kraje.

Výhody

- Naplnění požadavků ZKB
- Naplnění běžných standardů kybernetické bezpečnosti

Nevýhody

- povinnost zajistit udržitelnost
- navýšení provozních nákladů
- náročné na finanční a personální zdroje včetně organizace zvyšování kvalifikací

S ohledem na skutečnost, že bezpečnost informačních systémů kraje vyplývá z legislativního rámce, byla **zvolena investiční varianta**, která řeší jak oblast bezpečnosti informačních systémů a je v souladu s ICT strategií Pardubického kraje.

5.8. Možnost alternativních řešení (uvést zdůvodnění, pokud nejsou relevantní)

Z důvodu potřeby naplnění požadavků Zákona o kybernetické bezpečnosti České Republiky 181/2014 Sb., a splnění všech parametrů vyžadovaných prováděcí vyhláškou č. 316/2014 sb. nelze zvažovat Nulovou variantu.

Pro naplnění požadavků Zákona o kybernetické bezpečnosti byla hledána i alternativní řešení. Popis alternativních řešení je uveden v následujících odstavcích.

5.8.1. Alternativní řešení pro opatření – Provedení GAP analýzy

Pro ověření detailního aktuálního stavu připravenosti úřadu na plnění požadavků zákona o kybernetické bezpečnosti lze použít vícero metod:

Varianta 1: Využití Analýzy rizik úřadu

Jako stanovení vstupního stavu je možné využit analýzu rizik, kterou má úřad zpracovánu a její výstupy ve formě nápvrhu opatření a plánu zvládání rizik.

Výhody

- Nevyžaduje další cenové náklady

- Je k diapozici ihned

Nevýhody

- Rozsah ISMS neodpovídá plně rozsahu ve smyslu ZKB
- Neodráží zcela aktuální stav

Varianta 2: Zpracování detailní analýzy rizik

Vypracování GAP analýzy aktuálního stavu připravenosti nezávislým „auditorem".

Výhody

- Rozsah zkoumaného ISMS lze plně přizpůsobit požadavkům studie a ZKB
- Výsledek je aktuální ke dni ověření, které je blízké realizaci následných fází projektu
- Výstupy z analýzy je možno překlopit do zadání pro další fáze projektu

Nevýhody

- Vyžaduje cenové náklady
- Je třeba počítat s dobou nutnou na šetření a zpracování analýzy

Vybraná varianta a zdůvodnění jejího výběru

Vybrána byla varianta 2 – Provedení GAP analýzy a to proto, že výhody přesnosti a aktuálnosti společně s možností využití v rámci zadání a podkladů pro konfigurace zařízení převyšují nutnost vynaložení finančních prostředků.

5.8.2. Alternativní řešení pro opatření č. 1 - Implementace správy privilegovaných uživatelů a účtů

Pro zajištění požadavků a dodržení nápravných opatření je nutné nasadit řešení ze skupiny označované jako Privilege Identity Management, které obsahují všechny potřebné nástroje a funkce, nutné pro zajištění navržených opatření.

Hlavní komponenty řešení jsou:

- Centrální úložiště privilegovaných identit a údajům k nim (uživatelská jména, hesla, klíče)
- Centrální řízení přístupu k těmto identitám pouze schváleným uživatelům a aplikacím
- Komplexní audit při používání privilegovaných účtů
- Zajištění záznamů o činnostech privilegovaných uživatelů na kritických částech infrastruktury a v aplikacích ve formě session recordingu (jak grafické tak shell rozhraní)

Na trhu existuje poměrně úzká skupina možných řešení, které pokrývají všechna nutná opatření, a vzájemně se liší hlavně funkčními požadavky. Mezi tyto řešení patří:

- CA Privileged Access Manager
- Centrify Privileged Identity Management
- CyberArk Privileged Identity Management
- IBM Security Privileged Identity Manager

Požadavky na „Řešení":

- Zajištění identifikace a správa všech správcovských účtů
- Řízení a správa centrální bezpečnostní politiky pro privilegované a správcovské účty aplikací, databází, uživatelů a zařízení
- Poskytování privilegovaných přístupů a hesel k systémům pouze pro oprávněné administrátory na základě pověření
- Vytváření záznamů (logů) o činnosti administrátorů a nad kritickými systémy a aplikacemi ve formě video nahrávky a textového přepisu
- Automatické změny hesel privilegovaných účtu v definovaných časových intervalech anebo jednorázové po přístupu
- Zajištění kontrola minimální formy hesel účtů
- Zabezpečení nemožnosti vypnutí bezpečnostních pravidel a ochran privilegovanými uživateli (administrátory)
- Centrální nastavování oprávnění přístupu k systémům a aplikacím pro jednotlivce a skupiny uživatelů
- Zabezpečení dostatečně bezpečného úložiště aplikačních a systémových přihlašovacích údajů
- Realizace autentizace aplikací na základě parametrů (cesta, uživatelské jméno, IP adresa)
- Zabezpečení lokálních cache přihlašovacích údajů
- Autentizace do systémů s dvoufaktorovou autentizací, single sign on, AD (active directory)
- Samotné řešení nesmí poskytovat informace výrobci ani nikomu jinému bez souhlasu Zadavatele

5.8.3. Alternativní řešení pro opatření č. 2 - Implementace VPN brány

Z hlediska zvažovaných alternativ se hodnotilo několik hledisek pro výběr optimální varianty pro VPN bránu. Tyto parametry byly voleny dle prostředí zákazníka, odborností jeho správců, aktuálních a do budoucna predikovatelných bezpečnostních hrozeb, zákonných požadavků a aktuálních trendů.

- Bezpečnost

Podpora mobilních VPN skrze SSL.

Dále „LAN to LAN“ IPSec.

Z hlediska šifrovací algoritmů a protokolů je u IPSecu požadováno IKE verze2 a podpora SHA2

hash funkcí, a to včetně SUITE B šifrovacích algoritmů.

Veškeré výše požadované vlastnosti jsou RFC standardy.

- Integrace vůči stávajícímu prostředí

Stávající síť zákazníka využívá pro řízení SSL VPN přístupu Cisco ISE. Z těchto důvodů je požadována kontrola stavu koncového zařízení uživatele, který se připojuje pomocí SSL VPN oproti Cisco ISE, možnost vložení koncového zařízení do karantény při nesplnění bezpečnostních kritérií, možnost změny VPN profilu koncové stanice s využitím funkcionality "change of authorization". Možnost napojení na OTP.

Varianta 1 - Cisco ASA 5516-FPWR

Výhody

- Plně vyhovuje všem požadovaným vlastnostem z pohledu bezpečnostních funkcí
- Podpora šifrovacích algoritmů dle požadavků ZKB
- Kompatibilita se stávajícím prostředím
- Snadný převod konfigurace ze stávajícího řešení
- Stávající administrátoři jsou vyškoleni na tento typ zařízení, protože původní [redacted] se konfiguruje obdobným způsobem.

Varianta 2 – CheckPoint Firewall

Výhody

- Plně vyhovuje všem požadovaným vlastnostem z pohledu bezpečnostních funkcí
- Podpora šifrovacích algoritmů dle požadavků ZKB

Nevýhody

- Je zde nedostatek z hlediska nekompatibility se stávajícím prostředím, protože je provoz řízen skrze ISE server a funkci Change of Authorization. Tato funkce není podporovaná. Nasazení tohoto prvku by znamenalo změnu koncepce a přenastavení řízení přístupu do sítě.
- Náročnější převod konfigurace ze stávajícího řešení.
- Nutnost vyškolit obsluhu tohoto řešení.

Toto není doporučovaná varianta, protože nesplňuje veškeré technické požadavky. Dále jsou zde i vyšší pořizovací a provozní náklady.

Varianta 3 – Cisco ASA 5525-FPWR

Výhody

- Plně vyhovuje všem požadovaným vlastnostem z pohledu bezpečnostních funkcí
- Podpora šifrovacích algoritmů dle požadavků ZKB
- Kompatibilitou se stávajícím prostředím
- Snadný převod konfigurace ze stávajícího řešení
- Stávající administrátoři jsou vyškoleni na tento typ zařízení, protože původní [redacted] se konfiguruje obdobným způsobem.

Nevýhody

- Cena vstupní investice i provozní podpory

Toto není doporučovaná varianta, přestože splňuje veškeré požadavky. Důvodem jsou vyšší pořizovací i provozní náklady. Sice nabízí toto řešení vyšší výkon, ale pro požadovanou funkci je tento výkon zcela zbytečný.

Zvolené řešení

Zvolené řešení **Cisco ASA 5516-FPWR** splňuje veškeré klíčové technické požadavky a zároveň se jedná o variantu,

která patří do průměru z hlediska finanční náročnosti. Navíc nebude nutné zásadně investovat do vzdělání IT obsluhy a do implementace řešení, protože se využijí znalosti a konfigurace ze stávajícího prostředí

5.8.4. Alternativní řešení pro opatření č. 3 - Zajištění redundance optických tras pro přístupové switche

Pro zajištění redundantního připojení přístupových přepínačů neexistuje žádná úřadem aplikovatelná varianta. Využití bezdrátových přenosů je díky požadovaným technickým vlastnostem (datová kapacita, rychlost, latence, ...) nerealizovatelné, proto je k diskuzi pouze vedení kabelových tras a počty vláken.

5.8.5. Alternativní řešení pro opatření č. 4 – Doplnění přístupových přepínačů

Problematika obměny a doplnění přepínačů se dělí na několik kategorií:

Doplnění karet a rozhraní pro zajištění topologie ve vysoké dostupnosti

Zde se musí principiálně jednat o karty a moduly, které jsou definovány výrobcem stávajícího řešení. Nemohou se zde tedy hodnotit alternativy. Dojde k rozšíření dvou páteřních přepínačů o 8 portové 10 Gbps datové karty, které umožní zbudovat redundantní trasy z přístupových přepínačů na páteřní přepínače. Součástí návrhu jsou i moduly (transceivery) na stranu páteřních i desktopových přepínačů.

Obměna zastaralých přepínačů, které jsou mimo podporu výrobce.

Síť obsahuje přepínače [redacted], které jsou již mimo podporu výrobce a zároveň nemají podporu 802.1x pro ověřování klientských stanic a řadu dalších bezpečnostních funkcí (ARP inspekce, DHCP snooping atd.). Z hlediska zvažovaných alternativ se hodnotilo několik hledisek pro výběr optimální varianty pro nové přepínače. Tyto parametry byly voleny dle prostředí zákazníka, kvalifikací jeho správců, aktuálních a do budoucna predikovatelných bezpečnostních hrozeb, zákonných požadavků a aktuálních trendů. Níže jsou zmíněny nejvíce klíčové parametry.

Doplnění o dvojici přepínačů s podporou MAC SEC

Doplnění o dvojici přepínačů podporujících MAC SEC, které zajistí transparentní zašifrování 1Gbps datového spoje mezi centrální sítí a spisovnou. Spisovna je umístěna ve vzdálené lokalitě a provoz je zasílán po pronajmutém optickém vlákně. Náplní zaměstnanců umístěných v lokalitě spisovny je primárně praceí s VIS.

- **Bezpečnost**
  - Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)
  - RADIUS CoA
  - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní
  - Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX
  - TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)
  - Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru
  - Bezpečnostní funkce umožňující inspekci provozu protokolu ARP
  - Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy

- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)
- Posílání stavu stanice v Radius AV-Pair
- Možnost automatické aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)
- Podpora 802.1AE

- **Integrace vůči stávajícímu prostředí**

Stávající síť zákazníka již využívá ve své většinové části 802.1x ověřování uživatelů, přidělování VLAN (autorizace) a kontrolu stavu koncových zařízení (posture). Pro ověřování se využívá soustava Radius serverů na bázi Cisco ISE. Je vyžadována plná kompatibilita vůči aktuálnímu stavu, kdy nové přepínače musí plně podporovat stávající funkce a jejich nasazení nesmí mít vliv na stávající implementaci 802.1x.

- Ve stávajícím prostředí se na řadě lokalit využívají nekonfigurovatelné „low cost“ přepínače, které vyžadují multi-domain ověřování. Obdobnou funkci vyžaduje i implementovaná IP telefonie.
- Dále se bude využívat NetFlow protokol pro bezpečnostní analýzu provozu a je tedy nutné použít nesamplovanou verzi NetFlow (nebo ekvivaletního protokolu) protokolu.
- Vzhledem k profilaci zařízení a řízení přístupu podle stavu stanice je nutná funkce „Change of Authorization“, která zajistí vynucen změny stavu portu přepínače na základě aktuální kondice koncového zařízení.
- Je požadována možnost vložení koncového zařízení do karantény při nesplnění bezpečnostních kritérií a také možnost změny VLANy koncové stanice s využitím funkcionality "change of authorization".

Varianta 1 - Cisco přístupové přepínače a Cisco rozšiřující karty

Tato varianta splňuje veškeré požadavky jak z pohledu technických požadavků, tak i z pohledu kompatibility se stávajícím prostředím.

Do dvojice páteřních přepínačů se v této variantě doplní vždy jedna 10Gb rozšiřující karta s 8 porty do každého z nich. Tato karta bude sloužit pro vytvoření redundantních cest z přístupových přepínačů.
Zde není technicky možná alternativní nabídka od jiného výrobce.
Dále byly navrženy obměny výrobcem nepodporovaných přepínačů [redacted] Byly zde místo nich navrženy přepínače společnosti Cisco.
Výhody:

- Zachování původních konfigurací nebo jejich mírná obměna
- Kompatibilita se stávající koncepcí LAN sítě
- Není nutné celkové přeškolení administrátorů na zcela odlišnou technologii

- Lze využít již zakoupené Cisco ISE pro 802.1x, aniž by se muselo zásadně modifikovat jeho nastavení
- Je konfigurovatelné pořadí autentizačních metod u 802.1x (Dot1x, MAC based, Web Autentizace), což umožňuje zachovat stávající filosofii 802.1x ověřování
- Jednotné bezpečnostní politiky 802.1x skrze celou LAN síť

Tato varianta je doporučovaná, protože splňuje veškeré technické požadavky a zároveň je variantou nejlevnější.

Varianta 2 - HP přístupové přepínače a Cisco rozšiřující karty

Tato varianta je kombinovaná, kdy se využívají Cisco rozšiřující karty 10 Gb v páteřní části sítě. Pro přístupové přepínače se použily přepínače společnosti HP jako náhrada nepodporovaných přepínačů [redacted]

Nevýhody:

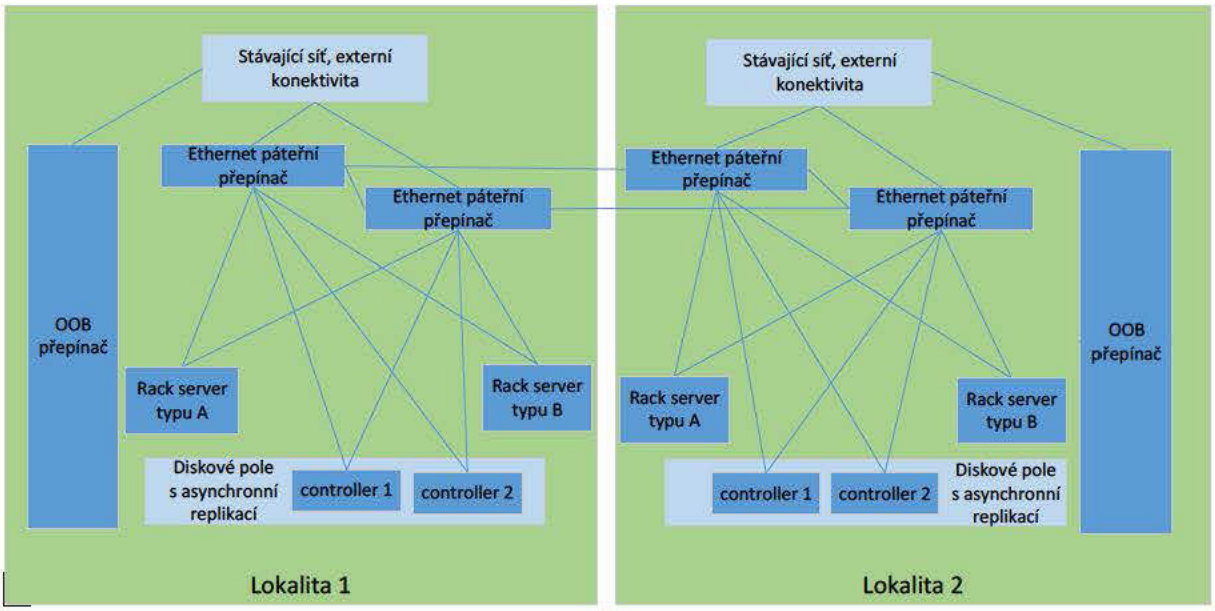
- Je nutné vytvořit zcela novou konfiguraci přepínačů a provést přemapování nastavení mezi různými výrobci
- Je nutné celkové přeškolení administrátorů na zcela odlišnou technologii
- Sice lze využít již zakoupené Cisco ISE pro 802.1x, ale je nutný jeho upgrade na poslední verzi a je nutné si vytvořit zcela odlišnou koncepci konfigurace.
- Není konfigurovatelné pořadí autentizačních metod u 802.1x (Dot1x, MAC based, Web Autentizace), což neumožňuje zachovat stávající filosofii 802.1x ověřování
- Musí se rekonfigurovat stávající část přepínačů a je nutné změnit bezpečnostní politiky 802.1x v celé LAN síti

Tato varianta není doporučovaná, protože je složitější při implementaci, má vliv na nastavení i ostatních přepínačů a Cisco Identity Serverů a je finančně náročnější.

5.8.6. Alternativní řešení pro opatření č. 5 - Doplnění HW Datového centra o servery a pole

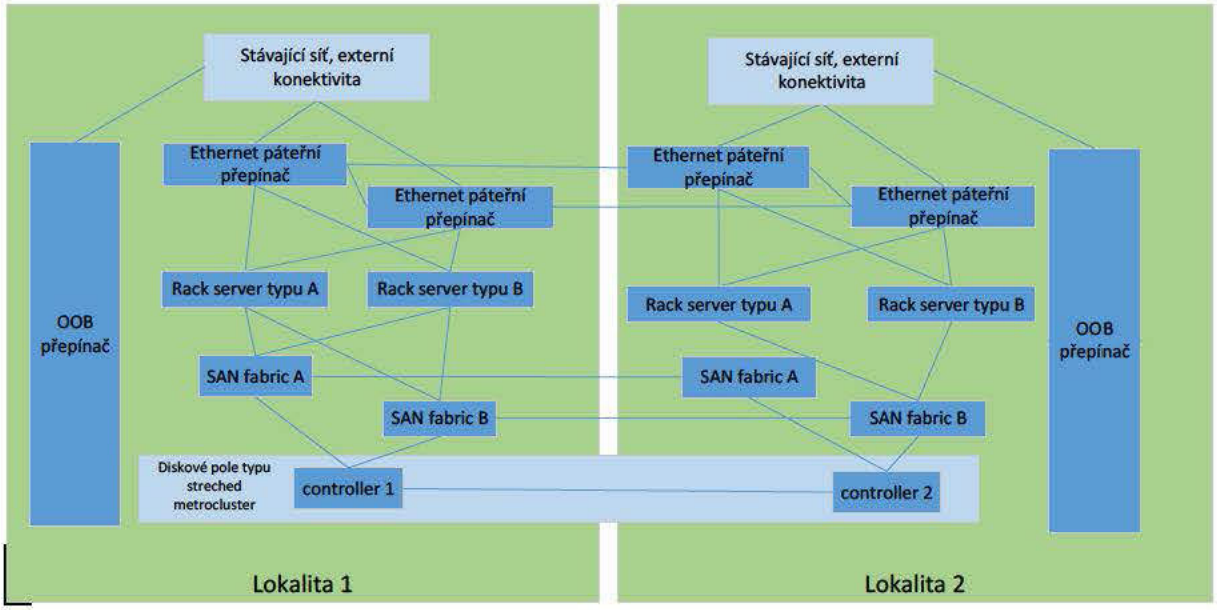
Při výběru řešení prostředků datového centra byly zvažovány následující řešení:

Disková pole s asynchronní replikací bez SAN sítě



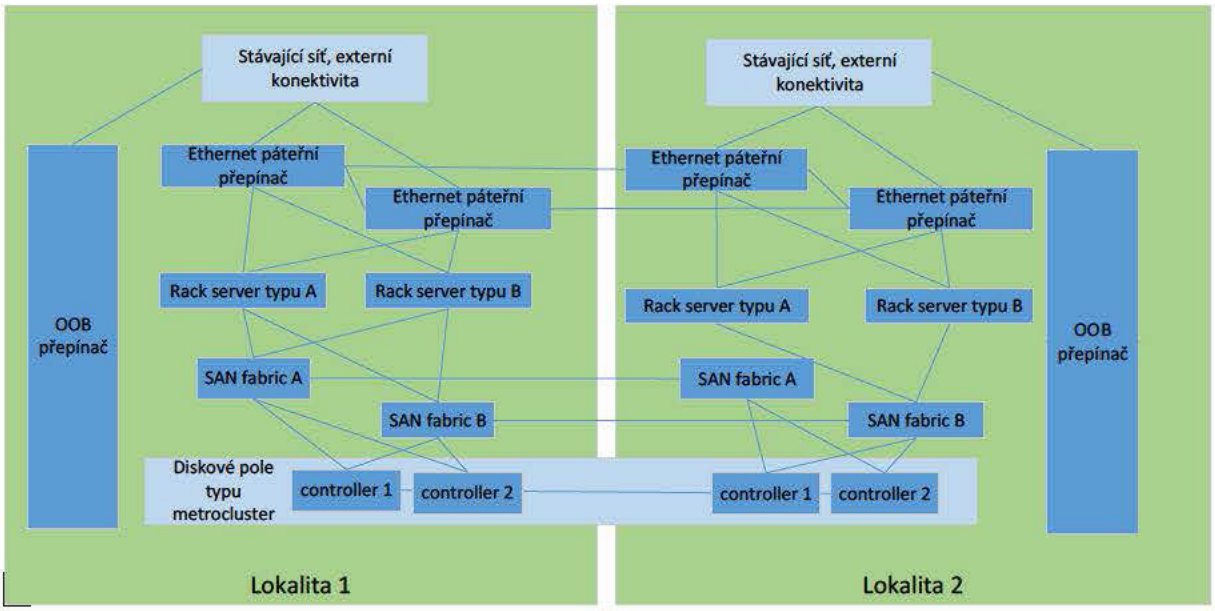
Obrázek 4 - Disková pole s asynchronní replikací bez SAN sítě

Streched metrocluster využívající FC SAN síť



Obrázek 5 - Streched metrocluster využívající FC SAN síť

Metrocluster využívající FC SAN síť



Obrázek 6 - Metrocluster využívající FC SAN síť

Pro výběr varianty byla zohledňována následující kritéria:

- Bezpečnost
  - Oddělení frontend a backend provozu
  - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní
  - Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX
  - TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)
  - Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru
  - Bezpečnostní funkce umožňující inspekci provozu protokolu ARP
  - Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy
  - Šifrování dat v diskovém systému na úrovni HW
  - Vysoká granularita přidělování oprávnění k různým zdrojům diskového systému
- Vysoká dostupnost
  - Zachování funkčnosti při poruše jednotlivé komponenty
  - Množství ztracených dat při poruše komponent nebo při výpadku celé lokality (minimální hodnota RPO – Recovery Point Objective a RTO – Recovery Time Objective)
  - Rychlost obnovy zašifrovaných dat při Ransomware útoku
- Integrace vůči stávajícímu prostředí
  - Stávající síť zákazníka využívá řešení oddělené LAN a SAN síť. SAN síť je postavená na FC protokolu s využitím přepínačů společnosti [redacted] využívána stávajícími servery a diskovými poli. Kombinování FC SAN přepínačů různých výrobců do společné fabriky je nedoporučované z důvodu nekompatibility. Zároveň je požadováno, aby bylo možné přistupovat k datům ze stávajícího prostředí na nové a obráceně.
  - Možnosti propojení lokalit, počet dostupné kapacity optických propojů

- Stávající síť zákazníka využívá virtualizační platformu společnosti [redacted] a je požadováno z důvodu jednoduchosti správy a jednotných politik připojení nových serverů pod společný management [redacted]

Obecná varianta 1 - Disková pole s asynchronní replikací bez SAN sítě

Výhody:

- Menší počet zařízení a tím pádem nižší cena z důvodu nevybudování separátní FC SAN sítě

Nevýhody:

- Oddělení frontend a backend provozu je realizováno ve formě různých logických VLAN sítí nikoliv na úrovni fyzických zařízení
- RPO v závislosti nastavení intervalu replikace, ale obecně minimálně 1 minuta
- RTO není jednoduše definovatelné a bude se pohybovat v řádech hodin
- Řešení neumožňuje komunikaci ke stávajícímu řešení bez výrazného zásahu do stávajícího řešení

Obecná varianta 2 – Stretched metrocluster využívající FC SAN síť

Výhody:

- Nižší cena oproti plnohodnotnému metro cluster řešení
- RPO dosahuje hodnoty 0
- RTO je možné dosáhnout v řádu minut
- Oddělení frontend a backend provozu ve formě dvou nezávislých sítí LAN a SAN
- Možnost komunikace se stávajícím řešením využívajícím stejnou architekturu oddělené LAN a SAN bez výrazné rekonfigurace

Nevýhody:

- Nižší úroveň redundance na lokalitě z pohledu diskového systému – pouze jeden řídící kontrolér. Při výpadku kontroléru dochází ihned k failover do druhé lokality, což zvyšuje zatížení sítě, nevede však k výpadku diskového systému.

Tato varianta se jeví jako nejvýhodnější z pohledu technického řešení a zároveň levnější variantu oproti variantě plnohodnotného clusteru.

Obecná varianta 3 – Metrocluster využívající FC SAN síť

Výhody:

- Nižší cena oproti plnohodnotnému metro cluster řešení
- RPO dosahuje hodnoty 0
- RTO je možné dosáhnout v řádu minut
- Oddělení frontend a backend provozu ve formě dvou nezávislých sítí LAN a SAN
- Možnost komunikace se stávajícím řešením využívajícím stejnou architekturu oddělené LAN a SAN bez výrazné rekonfigurace
- LAN přepínače podporují monitorování informací o tocích dat

Nevýhody:

- Vyšší cena oproti variantě stretched metrocluster

Konkrétní příklad varianty 2 – Stretched metrocluster postavený na technologii Netapp, síťová infrastruktura a výpočetní prostředky postavené na technologii Cisco Systems

Výhody:

- Tato řešení splňuje veškeré požadavky jak z pohledu technických požadavků (bezpečnosti, vysoké dostupnosti), tak i z pohledu kompatibility se stávajícím prostředím.
- RPO dosahuje hodnoty 0
- RTO je možné dosáhnout v řádu minut
- Oddělení frontend a backend provozu ve formě dvou nezávislých sítí LAN a SAN
- Možnost komunikace se stávajícím řešením využívajícím stejnou architekturu oddělené LAN a SAN bez výrazné rekonfigurace
- LAN síť je postavená na stejném výrobci jako zbylá síťová zařízení - není nutné celkové přeškolení administrátorů na zcela odlišnou technologii, kompatibilita se stávající koncepcí LAN sítě, na kterou budou prostředky datového centra připojeny
- SAN síť je postavená na přepínačích stejného výrobce, čímž je garantována kompatibilita v rámci FC fabriky a není nutné obnovovat všechny stávající FC SAN přepínače
- Řešení diskového systému zajišťuje jednak diskovou kapacitu a zároveň aplikačně konzistentní backup

Nevýhody:

- Mezi lokalitami bude nutné zajistit multimode optická vlákna v počtu minimálně 24 kusů (12 párů)

Tuto variantu doporučujeme. Jedná se o konkrétní příklad obecné varianty 2, tedy stretched metroclusteru, vyhovuje všem kritériím a byla cenově nejvýhodnější.

Konkrétní příklad – Dvě disková pole s asynchronní replikací postavené na technologii HP, síťová infrastruktura postavená na technologii Cisco Systems a výpočetní prostředky postavené na technologii HP

Výhody:

- Tato řešení splňuje veškeré požadavky jak z pohledu technických požadavků (bezpečnosti, vysoké dostupnosti), tak i z pohledu kompatibility se stávajícím prostředím.
- LAN síť je postavená na stejném výrobci jako zbylá síťová zařízení - není nutné celkové přeškolení administrátorů na zcela odlišnou technologii, kompatibilita se stávající koncepcí LAN sítě, na kterou budou prostředky datového centra připojeny

Nevýhody:

- RPO v závislosti nastavení intervalu replikace, ale obecně minimálně 1 minuta, a je tedy vyšší než v předchozí variantě
- RTO není jednoduše definovatelné a bude se pohybovat v řádech hodin a je tedy vyšší než v předchozí variantě
- Oddělení frontend a backend provozu je realizováno ve formě různých logických VLAN sítí nikoliv na úrovni fyzických zařízení

Tuto variantu nedoporučujeme.

Zdůvodnění výběru dané varianty

Vybrána byla varianta 2 – Stretched metrocluster, která se s ohledem na požadavky a finanční možnosti úřadu jeví jako nejvýhodnější technické řešení, a zároveň jde o levnější variantu oproti variantě plnohodnotného clusteru.

5.8.7. Alternativní řešení pro opatření č. 6 – Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě

V rámci průzkumu trhu, a to i po diskuzi s výrobcem Cisco Systems s.r.o. nebyla nalezena žádná variantní aplikace, která by poskytovala stejné nebo alespoň podobné funkcionality. Vzhledem k tomu, že aplikace využívají API systému Cisco ISE a jde o programové vybavení, mohou být do doby realizace projektu tyto aplikace vyvinuty.

Navrhovaná aplikace MABKEEPER využívá API rozhraní, které nabízí Cisco ISE, k možnostem správy databáze MAC adres, které se využívají k ověřování v síti pomocí protokolu 802.1x. Aby byl uživatel schopen komunikace s databází Cisco ISE, musí se do aplikace MABKEEPER přihlásit a mít dostatečné oprávnění k zápisu do definované skupiny MAC adres. K tomu slouží integrace aplikace pomocí LDAP konektoru s identity databází. Aplikace MABKEEPER je jedinečná, neboť kombinuje vlastnosti řízení přístupu pomocí oprávnění definované v externí databázi a komunikuje s Cisco ISE pomocí API rozhraní.
Pro monitoring sítě podléhající 802.1x je důležitá v přístupu zpracování údajů i druhá aplikace, OFFICELOCATOR. Aplikace je schopna získávat logy generované síťovými přepínači a Cisco ISE, na základě kterých dodává ucelené informace o stavu koncových stanic a uživatelů přihlášených do sítě.

AleFIT MAB Keeper

Aplikace AleFIT MAB Keeper umožňuje spravovat některá nastavení autentizačního systému bez přímého přístupu do jeho konfiguračního rozhraní. Aplikace díky několika modulům pokrývá různé případy užití, díky nimž je možné řešit problémy, které se typicky mohou vyskytnout po implementaci 802.1x kvůli chybějícím nebo nekompatibilním IT procesům. MAB Keeper obecně slouží pro správu MAC adres zařízení, které se v autentizačním systému používají pro autentizaci zařízení a nejsou kompatibilní se standardem 802.1x (tiskárny, IP telefony aj.) nebo pro správu MAC adres zařízení, u nichž se MAC adresa používá pro autentizaci. Takovým zařízením je vytvořena výjimka pro přístup do sítě díky přidání do autentizačního systému. Ke každé výjimce jsou evidovány různé informace, které usnadní případný troubleshooting nebo rozhodování o dalším prodloužení výjimky.
Mimo pasivních zařízení a zařízení, která se z libovolného důvodu nemohou autentizovat, umožňuje aplikace spravovat a kontrolovat přístup zařízení, u nichž je MAC adresa využita jako náhradní způsob autentizace. Typicky se jedná o zařízení konzultantů, která potřebují po určitou dobu přístup do firemní sítě, nebo o BYOD zařízení zaměstnanců. U takových výjimek je navíc evidován Sponsor, který připojení zařízení do sítě schválil a nese příslušnou odpovědnost. Speciálním případem je možnost zablokování přístupu pro určité zařízení a to buď jako preventivní opatření, nebo v rámci reakce na hrozbu, kterou pro síť již připojené zařízení představuje. V závislosti na účelu může být výjimka časově omezená, taková je po uplynutí stanoveného času z aplikace i autentizačního systému odmazána bez nutného zásahu administrátora.
Nad každou operací, kterou aplikace vykoná automaticky a nad každým úkonem, který vykoná uživatel přes

rozhraní aplikace, je veden detailní log. Ten napomůže případnému troubleshootingu či security auditu. Přístup do jednotlivých modulů aplikace je možné řídit na základě definovaných rolí uživatelů díky jejich členství ve skupinách v Active Directory.

AleFIT Office Locator

Aplikace AleFIT Office Locator představuje helpdeskový portál, který slouží k monitoringu a analýze 802.1x autentizace a poskytuje oprávněnému uživateli informace z různých zdrojů potřebné pro určení příčiny problému s autentizací či řešení incidentu v jednoduchém webovém rozhraní. Aplikace registruje jednotlivé autentizační relace a prezentuje jejich stav spolu s dalšími informacemi z Cisco ISE, Active Directory a síťových přepínačů. Uživatel tak má možnost si například zkontrolovat účet uživatele v Active Directory či konfiguraci portu na přepínači, aniž by měl do těchto systémů přímý přístup. Dostupnost různých funkcionalit je řízena díky členství uživatelů ve skupinách v Active Directory.
Obě aplikace jsou vzájemně integrované a pro některé funkcionality si navzájem poskytují potřebná data.
Výhody:

- možnost výjimky pro přístup do sítě časově omezit a nechat aplikaci automaticky odmazávat
- omezení přístupu do aplikací dle definovaných rolí uživatelů
- různé role pro konfigurační rozhraní Cisco ISE, síťových přepínačů i Active Directory
- možnost customizace aplikací i uživatelského rozhraní pro specifické potřeby zákazníka
- dostupnost informací z různých zdrojů potřebných pro troubleshooting a řešení problémů

Zdůvodnění výběru dané varianty

Z důvodu absence jiných aplikací, které by v době posuzování splňovaly požadovanou funkcionalitu byly pro naplnění požadavků vybrány aplikace MABKEEPER a OFFICELOCATOR. Obě aplikace splňují požadavky, jejich správa nepřináší pracovníkům IT zadavatele žádné zvýšení nároků na jejich kapacity a jejich provoz nepřináší zadavateli výrazné cenové nároky.

5.8.8. Alternativní řešení pro opatření č. 7 – Centrální logovací nástroj

Pro naplnění požadavků je možné realizovat ve třech úrovních dle zvolených řešení, od základních nástrojů pro jednoduché ukládání logů z prostředí po pokročilé SIEM řešení. Mezi vhodná řešení patří následující řešení:

- Balabit (syslog-ng)
- Qradar
- HPE ArcSight
- Splunk

Každé řešení má svojí samostatnou architekturu a jinou filozofii fungování, nelze je tedy přímo porovnávat, existují tři základní modely nasazení těchto řešení:

Centrální Syslog server

zajištění základního ukládání auditní stopy a jejich sběr z celé infrastruktury
Výhody:

- Jednoduché a levné řešení

Nevýhody:

- Není garantované nezpochybnitelné uložení logů
- Chybí podpora nástrojů pro složitější reporting a bezpečnostní dohled
- Logy jsou ukládané nestrukturovaně, omezené možnosti vyhledávaní
- Komplikovaná správa složitějšího prostředí, většího objemu logů

Log management s pokročilými funkcemi

Výhody:

- Podpora sběru standardních zdrojů logů od výrobce řešení (OS, DB, network, atd.)
- Centrální správa
- Garantované nezpochybnitelné uložení logů
- Pokročilé možnosti reportování a vyhledávání, notifikace
- Zpracování a ukládání strukturovaných logů

Nevýhody:

- Chybí pokročilé funkce pro detekci bezpečnostních incidentů

SIEM

Výhody:

- Komplexní řešení obsahující všechny funkce log managementu, a navíc pokročilé nástroje pro detekci bezpečnostních incidentů

Nevýhody:

- Finančně náročné řešení, jak z pohledu pořízení, tak údržby
- Technologicky a procesně velmi náročné na správnou implementace
- Komplexní správa, údržba a rozvoj řešení, vyžadující detailní znalosti fungování řešení

Zdůvodnění výběru dané varianty

Z hlediska potřeb a kompromisů z pohledu požadovaných funkcí a následných požadavků na provoz a dlouhodobý rozvoj řešení, jsme zvolili **Log Management** s pokročilými funkcemi s následujících důvodů:

- Jednoduchá implementace a provoz
- Dostatečné funkce centrální správu, podpora sběru logů a nástrojů pro reporting a vyhledávání
- Možnost garantovat neměnnost uložených logů
- Poměr dostupných funkcí a nákladů na pořízení a provoz
- Možnost licenčně rozšířit o funkce SIEM

5.8.9. Alternativní řešení pro opatření č. 8 - Implementace vysoké dostupnosti pro [redacted]

Z hlediska zvažovaných alternativ se hodnotilo několik hledisek pro výběr optimální varianty pro zajištění vysoké dostupnosti [redacted] databáze aplikace GINIS. Zvažovány byly nakonec dva způsoby řešení:

- Replikace na úrovni externích skriptů

- Nativní vysoká dostupnost, která je součástí [redacted] řešení

Varianta 1 – Sada externích skriptů

Tato varianta splňuje všechny technické požadavky.

Výhody:

- Není nutné upgradovat [redacted] databázi z verze [redacted]
- Jsou nižší provozní náklady
- Snadná implementace bez nutnosti migrace na [redacted]
- Není nutné investovat do rozšíření vzdělání administrátorů

Toto je doporučovaná varianta, protože splňuje veškeré požadavky a zároveň je i finančně nejvýhodnější.

Varianta 2 – [redacted]

Tato varianta nabízí nejlepší a nejsofistikovanější technické řešení.

Výhody:

- Online recovery databázových objektů
- Lepší správa datových toků než u varianty 1 a 2.
- [redacted]

Nevýhody:

- Značné pořizovací i provozní náklady (vyšší více než o řád oproti variantě 1)
- Nutnost upgrade [redacted] databáze z verze [redacted]
- Provést vyškolení administrátorů na složitější verzi produktu
- Provést převod databází při upgrade na [redacted] verzi

Toto není doporučovaná varianta, přestože splňuje veškeré požadavky a nabízí nejlepší technické řešení. Důvodem jsou výrazně vyšší pořizovací i provozní náklady (o více než jeden řád).

Zdůvodnění výběru dané varianty

Z hlediska potřeb řešení a cenové výhodnosti byla vybrána varianta 1 - Sada externích skriptů, která splňuje všechny požadavky.

5.8.10. Alternativní řešení pro opatření č. 9 - Implementace řešení pro monitorování toků

Pro monitorování toků existuje více nástrojů od různých výrobců. V této studii porovnáváme námi doporučované řešení společnosti Flowmon se dvěma konkurenčními řešeními.

Prvním z nich je Cisco Prime Infrastructure a druhé je StealthWatch.

Cisco Prime Infrastructure

Jedná se o nástroj pro správu a dohled Cisco zařízení. Kromě dohledu umožňuje zpracovávat i netflow data a na jejich základě umožňuje monitorovat datové toky v síti. Jedná se o robustní řešení podporující až 10 000 Cisco zařízení. Výhodou tohoto řešení je integrace monitorování datových toků se správou Cisco zařízení. Nevýhodou tohoto řešení je licencování na základě počtu a typu zařízení, které jsou tímto nástrojem spravovány a nemožnost integrace bezpečnostního řešení (např. analýza netflow záznamů pro identifikaci možných bezpečnostních incidentů).

StealthWatch

V současné době i tento produkt spadá do portfolia společnosti Cisco Systems. Jedná se o robustní nástroj na analýzu netflow dat pro detekci bezpečnostních incidentů. Tento nástroj umožňuje detekovat bezpečnostní incidenty ve velmi rozsáhlých sítích. Nevýhodou tohoto řešení je obtížnější analýza datových toků z hlediska provozního monitoringu a vysoké pořizovací náklady.

- Vyhodnocení alternativních řešení pro implementaci monitorování toků

Z hlediska zvažovaných alternativ se hodnotilo několik hledisek pro výběr optimální varianty pro monitorování toků. Tyto parametry byly voleny dle prostředí zákazníka, aktuálních a do budoucna predikovatelných bezpečnostních hrozeb, zákonných požadavků a aktuálních trendů.

- Monitorování toků

podpora zpracování různých formátů exportovaných dat – netflow, sFlow, jFlow, IPFIX
podpora viditelnosti do aplikační vrstvy – podpora NBAR2
zobrazení Top N statistik

- Bezpečnostní incidenty

na základě behaviorální analýzy detekovat možné bezpečnostní hrozby
upozorňovat na tyto hrozby pomocí generovaných notifikací

- Data Retention

uchovávání nasbíraných dat nejméně po dobu 6-ti měsíců
generování reportů o komunikaci uživatelů

- Zvolené řešení

Zvolené řešení splňuje veškeré klíčové technické požadavky a zároveň se jedná o variantu, která patří do průměru z hlediska finanční náročnosti.

5.8.11. Alternativní řešení pro opatření č. 10 – Doplnění redundantní [redacted] proxy

Z hlediska zvažovaných alternativ se hodnotilo několik hledisek pro výběr optimální varianty pro web proxy bránu. Tyto parametry byly voleny dle prostředí zákazníka, aktuálních a do budoucna predikovatelných bezpečnostních hrozeb, zákonných požadavků a aktuálních trendů.

Základní klíčové požadavky

- Licence pro minimálně 400 uživatelů
- Platnost podpory výrobce minimálně 5 let
- URL filtraci
- Antivirová kontrola
- Vysoká dostupnost řešení
- Každé zařízení musí mít dva napájecí AC zdroje
- Reputační databáze
- Propustnost minimálně 150 Mbps

Varianta 1 – Náhrada proxy brány [redacted]

Stávající proxy brána [redacted] bude nahrazena za [redacted].

Výhody

- Nedojde k obměně celého řešení, ale pouze jenom jedné komponenty
- Není nutné provádět složitou implementaci celého řešení, které může v případě jiného produktu trvat týdny
- Není nutné provést přeškolení obsluhy na jinou technologii
- Licence lze převést z původního zastaralého HW na nové zařízení

Stávají řešení pro ochranu uživatelského webového provozu je postaveno na [redacted] řešení, které se skládá z dvojice [redacted] proxy bran a nezávislých [redacted] antivirových branách.

Zastaralá [redacted] již není schopna plnit svoji funkci. Ve stávající architektuře je aktuálně nedostatek pouze v zastaralosti jedné proxy brány a ostatní komponenty plně vyhovují provozním i ZKB požadavkům. Je zcela zbytečné obměňovat celé řešení, ale stačí pouze nahradit jednu zastaralou proxy bránu

Varianta 2 – Nahrazení celého řešení za Cisco WSA

Cisco Web Security Appliances splňuje veškeré technické požadavky, ale je nutné obměnit řešení jako celek a není možné jím nahradit pouze jedinou zastaralou bránu.

Nevýhody:

- Musí dojít k obměně celého řešení včetně antivirových serverů a nepouze jenom jedné komponenty
- Je nutné provést implementaci proxy bran od začátku s tím, že politiky mezi [redacted] a Cisco WSA nejsou mezi sebou kompatibilní a je nutné je vytvořit znovu
- Je nutné provést přeškolení obsluhy na Cisco WSA technologii
- Nelze využít stávající licence z původního řešení

Tato varianta není doporučována, protože je finančně výrazně náročnější a nepřináší žádné zásadní výhody.

Vybraná varianta a její zdůvodnění

Doporučenou variantou je náhrada stávající nesuportované [redacted] novým typem zařízení [redacted] Toto řešení splňuje veškeré požadavky a zároveň je i finančně nejvýhodnější. Navíc nevyžaduje žádné další nároky na zaškolení obsluhy a migrace ze stávajícího typu je z pohledu administrace jednoduchá.

5.8.12. Alternativní řešení pro opatření č. 11 – Rozšíření [redacted] o SANDBOX

Z hlediska zvažovaných alternativ se hodnotilo několik hledisek pro výběr optimální varianty SandBoxu. Tyto

parametry byly voleny dle prostředí zákazníka, aktuálních a do budoucna predikovatelných bezpečnostních hrozeb, zákonných požadavků a aktuálních trendů.

Hlavní požadavky byly:

- Analýza minimálně 12 000 vzorků za 24 hodin
- Kompatibilita se stávajícím proxy systémem
- Vysoká dostupnost řešení (dvojice zařízení)
- Podpora výrobce minimálně 5 let
- Licence na bezpečnostní funkce na 5 let
- Lokální [redacted] bez nutnosti odesílání vzorků do cloudu
- Kombinace statické a dynamických technik pro analýzu malware
- Reputační filtry pro detekci malware
- Automatická aktualizace nových hrozeb z globální databáze výrobce
- Microsoft licence pro provoz v SandBoxu, pokud jsou potřeba

Varianta 1 – [redacted]

Toto řešení splňuje veškeré parametry, které jsou požadovány.

Výhody:

- Je možné vytvořit profil operačního systému dle reálného prostředí zákazníka
- Jedná se o řešení, které je z hlediska obsluhy méně náročné než ostatní varianty. „Velká“ SandBox řešení z hlediska náročnosti vyžadují dedikovanou obsluhu.
- Jednoduchou implementaci ve stávajícím prostředí
- Pouze se rozšíří znalosti o další komponentu stávajícího proxy řešení. Není nutné kompletní přeškolení.
- Jedná se o cenově nejvýhodnější variantu

Toto je doporučovaná varianta, protože splňuje veškeré požadavky a zároveň je i finančně nejvýhodnější.

Varianta 2 – Cisco Threat Grid

Výhody:

- Disponuje s rozsáhlými možnostmi v analýze zachycených podezřelých souborů. (řešení trajektorie souborů, retrospektivní analýza apod.)

Nevýhody:

- Neumožňuje vytvořit profily operačních systémů dle prostředí zákazníka
- Jedná se o velmi robustní nástroj, který vyžaduje:
  - sofistikovanou správu
  - dedikovanou obsluhu
  - rozsáhlé know-how pro využití potenciálů celého řešení
- úpravu stávající topologie při kontrole webového provozu
- přeškolení obsluhy na novou technologii

Toto není doporučovaná varianta, protože je pro stávající prostředí příliš komplikovaná z hlediska implementace, provozu a z důvodu vysokých pořizovacích i provozních nákladů.

Vybraná varianta

Jako nejvhodnější, a proto doporučovaná varianta se jeví implementace dvou boxů [redacted] s odpovídající licencí pro SandBox. Úřad již provozuje [redacted] proxy řešení, které je plánováno doplnit o nový redundantní box v opatření č. 11, proto se tato volba je vhodná i z hlediska administrace, protože navazuje na již využívané řešení a nevyžaduje rozsáhlé zaškolení obsluhy. Zároveň splňuje veškeré požadavky a je i finančně nejvýhodnější.

5.8.13. Alternativní řešení pro opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru

V průběhu studie bylo v rámci výběru vhodné varianty hodnoceno několik klíčových hledisek:

Webový aplikačí firewall

- Pozitivní a negativní bezpečnostní model
- Podpora HTTP/2
- Ochrana provozu typu Websocket
- Zabudovaná ochrana proti aplikačním DoS útokům
- Možnost vytvoření specifické ochrany, která není součástí, již zabudované ochrany (programovatelnost)
- Podpora importu ze skenerů třetích stran
- Logovaní a korelace událostí

Monitoring aplikací a vysoká dostupnost

- Monitoring dostupnosti služeb
- Podpora pro rozklad zátěže včetně aplikačního testování služeb
- SSL terminace vč. podpory šifer Camellia
- Podpora HTTP/2
- Podpora ECDSA a podpora hybridních certifikátů (DSA/ECDSA/RSA)
- Podpora pro HTTP Strict Transport Security (HSTS)
- Podpora akcelerace (Komprese, caching, optimalizace TCP stacku)
- Možnost vytvoření specifické operace s procházejícím provozem, která není součástí již zabudované funkcionality (programovatelnost), např. vkládání/odebírání HTML kódu, operace manipulace s daty, manipulace s HTTP záhlavím apod.

DoS ochrana

- Zařízení by mělo být optimalizováno pro ochranu před DoS útoky. Tradiční stavové zařízení (FW, IPS apod.) snadno podlehne celé řadě DoS vektorů
- Zařízení by mělo podporovat SSL terminaci pro inspekci aplikačních útoků
- Možnost rozšíření o další funkční celky např. možnost provádění autentizace uživatelů přistupující k webovým aplikacím
- Možnost vytvoření specifické ochrany, která není součástí, již zabudované ochrany (programovatelnost)

Varianta 1 - Citrix

Výhody:

- Podpora Multitenant prostředí na jedné HW applianci
- Poskytuje vyspělé funkce pro webové bezpečnost, včetně inspekce XML a JSON. NetScaler může transparentně přidat podporu HTTP 2.0 pro starší aplikace. Také to integruje řadu výkonných optimalizačních funkcí.
- Security Insight konzole podporuje real-time monitoring aktuálního stavu a možnosti pokročilé správy a výkonnostního monitoringu
- Poskytuje vysoký výkon, zvlášť v případě vysokého poměru SSL/TLS provozu
- Funkcionalita IP reputation je poskytována jako součást řešení bez dalších poplatků

Nevýhody:

- AppFirewall je primárně software komponenta jiného řešení (ADC- Application Delivery Controller) a primárním určením řešení není poskytování bezpečnostních funkcí, ale zajištění provozu a unifikace prostředí při provozování aplikací. Oproti ostatním výrobcům má velké mezery v poskytovaných bezpečnostních funkcích
- Řešení má velmi slabé auditní a reportovací funkce, spojené s nízkou kvalitou a vypovídající hodnotou auditního logu

Varianta 2 - F5

Výhody:

- Podpora WAF funkcí společně s ADC
- Podpora nasazení on-premise a cloud-based, včetně hybridního nasazení
- Vhodné rozšíření funkcí pro stávající zákazníky s ADC

Nevýhody:

- Komplikované úvodní nasazení spojené s konfigurací a výkonnostními problémy
- IP reputation, které je součástí řešení, má omezenou funkcionalitu proti jiným řešením a neposkytuje dostatečnou úroveň doplňujících informací
- Kvalita auditní stopy při řešení problémů není dostatečná a znesnadňuje rychlé a efektivní řešení.

Varianta 3 - Imperva

Výhody:

- Flexibilita řešení při architektonických změnách v prostředí a aplikacích
- Vysoká kvalita centrálního managementu které je vhodné pro všechny typy nasazení, včetně velkých prostředí
- Primární zaměření řešení na bezpečnostní funkce při ochraně všech typů aplikací
- Imperva je jasný leader při sledování a detekování útoků vůči aplikacím. Poskytuje detailní informace ke všem typům útoků a nejrychleji reaguje na nově vznikající hrozby

Nevýhody:

- Neposkytuje ADC funkcionality

Zvolené referenční řešení

Pro zajištění ochrany před aplikačními DoS útoky byla vybrána technologie F5 BIG-IP, která splňuje všechna

hlediska specifikovaná v textu výše. Řešení předpokládá vznik vrstvy abstrakce mezi klientem a serverem, pak realizována ochrana webových aplikací, monitoring a vysoká dostupnost aplikací a možná ochrana před aplikačními (web) DoS útoky. Zvolené řešení přináší možnost integrace jednotlivých vlastností do jednoho zařízení, případně jejich možnou kombinaci a zároveň možnost rozšíření o další funkční celky, které mohou být budoucnu využity např. licenční rozšíření o plnohodnotné DNS vč. funkce DNS firewallu nebo o autentizační bránu poskytující autentizační a služby (např. autentizace do webových aplikací, SSO, SAML, atd)

5.8.14. Alternativní řešení pro opatření č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS

V rámci tohoto opatření se neprovádělo hodnocení alternativních řešení od různých výrobců, protože se jedná o proprietární aplikaci. Její rozšíření o sběr transakčních logů, které zajistí soulad s prováděcí vyhláškou 316/2014, lze zajistit pouze modulem od tvůrce aplikace (společnost GORDIC spol. s r.o.). V následujících částech této kapitoly je pak hodnoceno, zda je tento modul nutný z pohledu naplnění Zákona o kybernetické bezpečnosti (viz. kapitola Identifikovaná rizika).

Systém GINIS nebyl principiálně navrhován v souladu se Zákonem o kybernetické bezpečnosti. Je to dáno tím, že vznikl výrazně dříve než tento zákonný požadavek. Navrhovaný rozšiřující modul je reakce tvůrce aplikace na zajištění kompatibility se ZKB a je jediným technickým řešením legislativních požadavků

Varianta 1 - Transakční protokol ADM s [redacted] konektorem

Modul pro transakční protokol ADM s [redacted] konektorem řeší funkční nedostatky vůči prováděcí vyhlášce 316/2014. A to z pohledu logování (§21) a také z pohledu používání doporučených šifrovacích algoritmů skrze síťové prostředí (§25).

Výhody

- Plně vyhovuje všem požadovaným vlastnostem z pohledu bezpečnostních funkcí
- Sběr transakčních logů z jednotlivých modulů systému GINIS dle § 21 vyhlášky 316/2014 kybernetické bezpečnosti
- Podpora exportu do syslog
- Detekce pokusů o neoprávněná přihlášení
- Možnost volby, jaké události systému se budou logovat
- Podpora exportu logu do SIEM
- Podpora exportu do PDF souborů (včetně el. podpisu a časového razítka)
- DB - Neúspěšné pokusy o přihlášení do DB
- Logování editace subjektu administrace
- Logování administrace přihlašovacích účtů
- Logování administrace parametrů
- Možnost nastavit automatické zrcadlení úložiště systému GINIS
- Přístup k úložišti [redacted] pomocí zabezpečeného protokolu
- Zajištění vysoké dostupnosti mezi GINIS aplikací a datovým uložištěm dokumentů

5.8.15. Alternativní řešení pro opatření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů

Viz. kapitola 5.8.15 Alternativní řešení pro opatření č. 14 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS.

5.8.16. Alternativní řešení pro opatření č. 15 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů

Nasazení dvoufaktorového ověřování významně zvýší kvalitu bezpečnosti z pohledu z §18 - Nástroj pro ověřování identity uživatelů prováděcí vyhlášky č. 316/2014 Sb.. Pro zajištění druhého faktoru autentizace je možno využít některou z následujících metod:

Token

Výhody

- Uživatel nepotřebuje znát heslo
- Funguje na principu časové značky

Nevýhody

- Neobsahuje certifikát
- Vysoká cena
- Nelze použít pro ověření v rámci fyzické bezpečnosti

Mobilní řešení ESET Secure Authentication

Výhody

- Používá dvou faktorové ověření s jednorázovým heslem (2FA OTP). (Heslo je náhodné, proto je nelze předvídat ani znovu použít)
- Snadná implementace pomocí navázání na RADIUS, API, nebo SDK
- Nevyžaduje žádný další HW na straně koncové stanice

Nevýhody

- Vyžaduje použití chytrých telefonů a jejich zařazení do centrálního nástroje vzdálené správy
- Nelze použít pro ověření v rámci fyzické bezpečnosti

Čipová karta

Výhody

- Lze použít pro ověření do počítače, OS, Aplikací, VPN
- Příznivá cena
- Lze využít jako vstupní karta v systému EKV, využije se tak stávající infrastruktura a výstupy předchozích projektu Pardubického kraje

Nevýhody

- Vysoká cena celého systému při novém pořízení (v případě KÚ neplatí, využijí prostředky předchozích projektů)

Vybraná varianta

Jako nejvhodnější ze zvažovaných variant byly zvoleny čipové karty, které dávají možnost jednoduché implementace, mají nízkou náročnost na provozní administraci, a navíc umožňují využití v rámci fyzické bezpečnosti v systému kontroly a evidence vstupů pro identifikaci administrátorů a oprávněných osob přistupujících do prostor ICT, ve kterých jsou umístěny významné informační systémy.

5.8.17. Alternativní řešení pro opatření č. 16 – Rozšíření stávajícího dohledového centra [redacted]

Pro zajištění monitoringu infrastruktury lze využít:

Nagios

Výhody

- Open Source
- Neplatí se pravidelná podpora

Nevýhody

- Složitý na administraci
- Nelze sjednat oficiální podporu, lze řešit pouze komunitní podporou

Solarwinds

Výhody

- Snadná implantace
- Rozsáhlé bezpečnostní řešení

Nevýhody

- Vysoká cena

[redacted]

Výhody

- Snadná instalace
- Úzká provázanost se systémem Windows
- Předpřipravené bezpečnostní senzory MS Windows
- Již odzkoušené funkční řešení v rámci úřadu
- Obsluha je zaškolena
- Snadná migrace na novou platformu

Nevýhody

- Platba pravidelné podpory
- Jde o placenou aplikaci

Vybraná varianta

Vybrána byla varianta využívající stávajícího [redacted] řešení a zvažována je pouze migrace na nový HW pro zisk výkonu dostatečnému i pro tento projekt. Nevyžaduje žádné další náklady na zaškolení a implementaci. Dostatečná funkcionalita splňující požadavky zákona.

5.8.18. Alternativní řešení pro opatření č. 17 - Implementace testovacího centra

Pro zajištění bezpečného provozu chybí v infrastruktuře vyhraněná část na otestování nasazení úplně nového software nebo případně jeho aktualizací s otestováním vlivu změn. Toto prostředí musí být bezpečně odděleno od zbytku sítě, ale dosažitelné administrátorům provozu, bezpečnosti i dodavatelských firmám přistupujím přes VPN.

Process Monitor

Process Monitor je pokročilý monitorovací nástroj poskytovaný zdarma společnostní Microsoft a distribuovaný v rámci balíku Windows Sysinternals. Nástroj umožňuje v reálném čase monitorovat dění na úrovni registrů, souborového systému, sítě a procesů (resp. vláken). Vzhledem k širokým možnostem filtrování detekovaných událostí by bylo požadovanou funkčnost možné s pomocí tohoto nástroje zajistit (omezením zobrazených informací na ty související s procesem instalované aplikace, případně jím vytvořené podprocesy). Bližší informace o nástroji Process Monitor jsou k dispozici na stránkách https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx.

Výhody

- Freeware
- Logování událostí i na úrovni sítě a procesů
- Široká podpora typů výstupních souborů

Nevýhody

- Nástroj je poskytován bez podpory
- Složitější ovládání
- Nástroj není primárně určen pro zamýšlené použití a získání všech potřebných informací by mohlo být v případě některých zkoumaných aplikací komplikované

Sandboxie

Nástroj poskytuje možnost spouštění aplikací ve virtuálním prostředí (sandboxu) a sledování jimi provedených změn na úrovni souborového systému a registrů. Nástroj je poskytován komerčně s cenou licence cca 50 USD/rok. Požadované funkčnosti by mělo být možné uvedeným řešením realizovat, jako potenciální omezení se jeví provádění změn pouze ve virtualizovaném obrazu operačního a souborového systému. Bližší informace o nástroji Sandboxie jsou k dispozici na stránkách https://www.sandboxie.com/.

Výhody

- Vysoká úroveň bezpečnosti při testování potenciálně škodlivých aplikací v důsledku jejich spouštění v sandboxu

Nevýhody

- Nekompatibilita s mnoha (především bezpečnostními) produkty
- Promítání změn pouze do virtuálního prostředí a tedy potenciální neschopnost detekovat případný vznik problému/konfliktu s jinou aplikací v reálném systému
- K dispozici je pouze licence s roční platností

SysTracer Pro

Nástroj SysTracer Pro umožňuje sledovat změny provedené na úrovni souborového systému, registrů a ovladačů. Nástroj je komerčně nabízen s cenou licence cca 50 USD. Principiálně je funkce nástroj založená na pořizování

snapshotů – obrazů stavu systému – a detekci změn, k nimž mezi nimi došlo. Pomocí popsaného mechanismu je možné relativně snadno determinovat změny, které provádí libovolná aplikace v rámci instalace/za běhu a pro zajištění požadovaných funkčností by tak byl přijatelný. Bližší informace o nástroji SysTracer Pro jsou k dispozici na stránkách http://www.blueproject.ro/systracer.

Výhody

- Licence pro nástroj je časově neomezená
- Možnost práce s více historickými snapshoty/práce se snapshoty z různých systémů
- Podpora vzdáleného získávání snapshotů

Nevýhody

- Bezplatná technická podpora a updaty pro aplikaci jsou omezeny na jeden rok, pro jejich zajištění na další roky je nutné pořídit jí zvlášť
- Omezený počet typů souborů s výstupy

Vybraná varianta

Jako nejvhodnější ze zvažovaných variant pro zajištění požadované funkčnosti se jeví použití nástroje SysTracer Pro. Aplikace je schopná pořizovat snapshoty stavu operačního a souborového systému a ty následně porovnávat s obrazy pořízenými historicky. Mimo jiné nástroj umožňuje monitorovat změny, k nimž došlo v oblasti spouštěných služeb a ovladačů, načtených DLL knihoven, otevřených síťových portů a instalovaných aplikací. Výstupy (výsledek porovnání snapshotů) je možné exportovat ve formátu HTML nebo PDF. V rámci jednotlivých pořízených obrazů je možné vyhledávat a nástroj poskytuje podporu pro export a import snapshotů. Dle nastavené licenční politiky je součástí licenčního poplatku vždy i roční technická podpora a updaty. Podporu a updaty pro nástroj po uplynutí roční lhůty je možné zajistit na další rok za čtvrtinovou cenu.

Zdůvodnění výběru dané varianty

Nástroj SysTracer byl pro zajištění požadované funkčnosti zvolen především vzhledem k tomu, že princip porovnávání snapshotů systému umožňuje velmi jednoduchým a přesným způsobem detekovat v podstatě libovolné změny, k nimž za běhu aplikace či při její instalaci došlo. Další nezanedbatelnou výhodou je časově neomezená licence nástroje, díky čemuž odpadá nutnost jejího periodického obnovování.

5.8.19. Alternativní řešení pro opatření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management

OpenVAS

Vulnerability management nástroj OpenVAS je open source řešení umožňující pomocí distribuovaných privilegovaných i neprivilegovaných skenů odhalovat zranitelnosti na koncových uživatelských systémech i serverech. Platforma se skládá z centrálního manažeru a jednoho či více skenerů, k nimž se manažer vzdáleně připojuje. Skeny webových aplikací je nástroj schopný provádět pomocí integrace s open source nástrojem w3af. Bližší informace o nástroji jsou k dispozici na http://openvas.org/.

Výhody

- Open source nástroj
- Neomezený počet skenovaných adres
- Neomezený počet uživatelů

- Neomezený počet skenerů

Nevýhody

- Chybí oficiální podpora pro agentské skeny
- Tradičně vyšší počet false-positive detekcí
- Absence některých pokročilých funkcí

Rapid7 Nexpose Express

Platforma Nexpose Express poskytuje široké možnosti skenování koncových systémů a serverů i webových aplikací. Umožňuje provádět vzdálené privilegované a neprivilegované skeny a aktuálně je vyvíjeno rozšíření pro umožnění agent-based skenů. Instalace je vždy lokální a podporuje distribuované skeny pomocí dvou skenerů umístěných v různých sítích. Licence jsou časově neomezené a obsahují cenu podpory a au na jeden rok Cena varianty umožňující skenování 128 IP adres je $2000, cena varianty umožňující skenování 256 adres pak $3000, je možné zajistit však licenci pro skenování až 1024 IP adres. Bližší informace o nástroji jsou k dispozici na https://www.rapid7.com/products/nexpose/download/editions/.

Výhody

- Časově neomezená licence
- Cíle pro skenování jsou omezeny pouze na počet licencovaných adres

Nevýhody

- Pouze jeden uživatelský účet
- Maximálně 2 skenery
- Podpora agent-based skenů aktuálně není plně implementována
- Bezplatná technická podpora a updaty pro aplikaci jsou omezeny na jeden rok, pro jejich zajištění na další roky je nutné pořídit jí zvlášť

Tenable Nessus Manager

Nessus Manager je distribuovanou vulnerability management platformou s lokálně instalovaným centrálním řídicím systémem, umožňujícím připojení libovolného počtu skenerů a podporujícím agent-based skenování pro usnadnění detekce zranitelností na noteboocích a dalších zařízeních, která nejsou dlouhodobě připojena k síti. Nástroj obsahuje vysoké množství modulů pro skenování různých operačních systémů, síťových zařízení i webových aplikací. Licence mají platnost jednoho roku a jsou standardně nabízeny ve verzi pro 128 IP adres ($2920), 256 IP adres ($4745) a 512 IP adres ($7665), licence pro vyšší počet skenovaných IP adres je však možné zajistit. Bližší informace o nástroji jsou k dispozici na http://www.tenable.com/products/nessus-vulnerability-scanner/nessus-manager.

Výhody

- Neomezený počet skenerů
- Počet agentů odpovídající počtu licencovaných IP adres
- Schopnost skenovat i větší počet IP adres než je licencován (v inkrementech limitovaných licencí)

Nevýhody

- Časově omezená licence

Vybraná varianta

Zejména s ohledem na časově neomezenou formu licence se – i přes prozatímní absenci agentských skenů – jako nejvhodnější řešení pro zajištění požadovaných funkčností jeví nástroj Rapid7 Nexpose Express. Nástroj je schopný realizovat distribuované skeny operačních systémů i webových aplikací a umožňuje pokročilým způsobem určovat nastavení těchto skenů. Skeny je rovněž možné spouštět v přednastaveném čase či se specifikovanou periodou. Implementaci je možné provést formou instalace na systém s OS Windows či Linux nebo formou virtuálního zařízení. Pro případ potřeby propojení nástroje s jiným systémem je k dispozici API rozhraní. Nástroj podporuje pouze jediného uživatele a maximálně dva různé skenery – připojení dalších skenerů není možné. Licence je, jak bylo uvedeno, časově neomezená a její součástí je podpora na období jednoho roku. Po prvním roce je možné za sníženou sazbu podporu dokoupit.

Zdůvodnění výběru dané varianty

Primárním důvodem pro doporučení nástroje Nexpose Express jako vhodného vulnerability management systému, je časová neomezenost licence při zachování relativně příznivých cenových podmínek. Vzhledem k tomu, že z pohledu funkčností je, až na absenci agent-based skenů, systém srovnatelný s konkurenčními řešeními, lze pro dlouhodobé používání výše uvedený argument považovat za dostatečně pádný.

5.9. Vymezení všech zainteresovaných subjektů a jejich členění

Zainteresovanými subjekty v rámci projektu "Bezpečnost komunikační infrastruktury" jsou cílové skupiny popsané v kapitole 6.3, "Žadatel" - Pardubický kraj (Komenského nám. 125, 532 11 Pardubice), "Zpracovatel studie" společnost ALEF NULA, a.s. (U Plynárny 1002/97, 101 00 Praha 10) a v přípravné fázi projektu bude zainteresovaným subjektem společnost, která bude vybrána k realizaci všech opatření projektu jako vítěz výběrového řízení.

6. Zdůvodnění potřebnosti realizace projektu

6.1. Stručné zdůvodnění záměru a jeho vazba na specifický cíl 3.2 Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality IKT

Realizace projektu vychází z povinnosti žadatele zajistit soulad se zákonem 181/2014. Sb., o kybernetické bezpečnosti, ve znění pozdějších a doprovodných předpisů. Projekt plně reflektuje Strategický rámec rozvoje veřejné správy České republiky pro období 2014 – 2020 schváleným usnesením Vlády České Republiky ze dne 27. srpna 2014 č. 680 (dále jen Rámec), konkrétně specifický cíl 3.2 Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality IKT. Projekt reaguje na zvyšující se potřebu řešení kybernetické bezpečnosti a váže se na realizaci jediného specifického cíle, kterým je dobudování informačních a komunikačních systémů veřejné správy a realizace bezpečnostních opatření podle zákona o kybernetické bezpečnosti. Hlavní podporovanou aktivitou je zabezpečení tzv. významných informačních systémů (dále jen „VIS“) a tzv. kritické informační infrastruktury (dále jen „KII“) veřejné správy dle zákona č. 181/2014. Sb., o kybernetické bezpečnosti, ve znění pozdějších a doprovodných předpisů. Pakliže by žadatel tento záměr nerealizoval, nejenže by se vystavil sankcím dle zmíněného zákona, ale především kybernetickým útokům, proti nimž není dostatečně zabezpečen.

6.2. Definice oblastí, které bude projekt řešit, a zdůvodnění priority jejich řešení (s uvedením vazby projektu na Strategický rámec rozvoje veřejné správy).

V souladu s § 28 odst. 1 zákona č. 181/2014 Sb., stanovily Národní bezpečnostní úřad a Ministerstvo vnitra aktuální přílohou č. 1 vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích Pardubický kraj jako správce těchto **Významných informačních systémů**:

PČ	*Název VIS*	*Popis*
107	**Integrovaný informační systém GINIS**	Modulární systém GINIS společnosti Gordic. Pokrývá oblasti rozpočtu, účetnictví, majetku, dotace, styk s bankami, smlouvy, spisová služba a další moduly související s provozem úřadu

Tabulka 8 Významný informační systém Pardubického kraje

Dotčený systém ani jeho moduly nepatří mezi systémy spadající pod ustanovení zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ani na ně nemá přímý vliv.
Kompletní popis současného stavu řešení je detailně popsán v kapitole 8. Řešení projektu je vizualizačně zachycen ve schématu níže. Východiskem pro zpracování řešení byl dokument „Strategický rámec rozvoje veřejné správy ČR pro období 2014-2020“ zpracovaný Ministerstvem vnitra, odborem strategického rozvoje a koordinace veřejné správy, a to především okruh číslo 7. Kybernetická bezpečnost.

6.3. Identifikace dopadů a přínosů projektu s důrazem na popis dopadů na cílovou skupinu

Pro identifikaci přínosů projektu Bezpečnost komunikační infrastruktury si zopakujme tabulku výstupů, kde jsou vidět cílové skupiny:

Vize projektu	Bezpečnost komunikační infrastruktury
Cílové skupiny/Subjekty zapojené do projektu	Krajský úřad a jeho zaměstnanci, občané a podnikatelé / organizace kraje, města a obce,
Přepokládané výstupy	Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti
Očekávané přínosy	Zabezpečený provoz souvisejících s výkonem veřejné správy v souladu s legislativou, které mimo jiné zajistí ochranu před kybernetickými útoky
Klíčové aktivity	Implementace technických opatření

Tabulka 9 Výstupy a přínosy projektu

Pro skupinu:

- Zaměstnanci Krajského úřadu Pardubického kraje budou přínosy:
  - Bezpečnost dat
  - Vysoká dostupnost systémů
  - stabilita ICT
- Zaměstnanci organizací zřizovaných Pardubickým krajem:
  - Bezpečnost dat
  - Vysoká dostupnost systémů
  - stabilita ICT
- Občané
  - vysoká dostupnost služeb (weby, ...)
- Fyzické i právnické osoby (podnikatelé)
  - vysoká dostupnost služeb (weby, ...)

Žádné z implementovaných technických opatření by nemělo přinést jakékoli negativní dopady na cílové skupiny projektu.

7. Management projektu a řízení lidských zdrojů

Kapitola popisující personální obsazení jednotlivých týmu, jejich pracovní náplně a požadované kvalifikace jednotlivých členů.

7.1. Popis činností a osob (kvalifikace, praxe), podílejících se na realizaci

V níže uvedené tabulce je vidět Projektový tým, struktura:

Funkce v rámci projektového týmu	Člen projektového týmu Funkce v rámci organizace	Zapojení ve fázi projektu
Garant projektu, vedoucí projektu	Ing. Roman Borkovec vedoucí oddělení informatiky, Pardubický kraj	Přípravná Realizační Provozní
Odborný garant projektu	Bc. David Rezler oddělení informatiky, Pardubický kraj	Přípravná Realizační Provozní
Odborný garant projektu	Ing. Jiří Poskočil oddělení informatiky, Pardubický kraj	Přípravná Realizační Provozní
Odborný garant projektu	Ing. Tomáš Číhař oddělení informatiky, Pardubický kraj	Přípravná Realizační Provozní
Odborný garant projektu	Miloš Zeman oddělení informatiky, Pardubický kraj	Přípravná Realizační Provozní
Administrátor projektu, projektový manažer	Ing. Vladimír Římánek Odbor rozvoje, Pardubický kraj	Přípravná Realizační Provozní
Konzultant	Ing. Jarmila Krejčí Regionální rozvojová agentura Pardubice	Přípravná
Finanční manažer	Ing. Pavlína Bečková Odbor rozvoje, Pardubický kraj	Přípravná Realizační Provozní

Funkce v rámci projektového týmu	Člen projektového týmu Funkce v rámci organizace	Zapojení ve fázi projektu
Právník projektu	Mgr. Pavel Menšl Vedoucí oddělení veřejných zakázek, Pardubický kraj	Přípravná Realizační Provozní

Tabulka 10 Projektový tým žadatele, struktura

Garant projektu, vedoucí projektu je osoba primárně zodpovědná za kontrolu projektu na úrovni managementu Pardubického kraje. Dále je zodpovědná za propagaci projektu na formální úrovni, tedy v médiích, při formálních příležitostech či směrem k občanům.

Náplň činnosti:

Přípravná fáze	Investiční fáze	Provozní fáze
• Propagace projektu • Podíl na definici projektu • Kontrola projektu na úrovni managementu kraje	• Propagace projektu • Kontrola projektu na úrovni managementu kraje	• Propagace projektu • Kontrola projektu na úrovni managementu kraje

Tabulka 11 Náplň činnosti garanta projektu (vedoucího projektu)

Odborný garant projektu je osoba projektového týmu, která komplexně vytváří cíle a směry projektu. Předmět projektu je postaven na odborných znalostech těchto osob. Jejich podněty jsou hlavními vstupy projektu. Hájí zájmy zadavatele, v průběhu realizace je zodpovědný za to, že zvolené postupy v projektových dokumentacích odpovídají technickým a procesním standardům a normám. Požadavkem odbornosti této role je zkušenost se supervizí a kontrolou projektu, stejně jako s provozem úřadu, znalostí jeho procesních norem. Manažerské zkušenosti a detailní znalosti problematiky je samozřejmostí.

Náplň činnosti:

Přípravná fáze	Investiční fáze	Provozní fáze
• Definování předmětu projektu • Spolupráce na přípravě a realizace výběrových řízení veřejných zakázek • Podíl na zpracování Studie proveditelnosti	• Spolupráce na přípravě a realizace výběrových řízení veřejných zakázek • Kontrola plnění technologických parametrů díla, kvality dodávky • Ochrana zájmů zadavatele • Kontrola procesních a technických standardů	• Kontrola a dohled nad provozní fází projektu • Zajištění udržitelnosti projektu

Tabulka 12 Náplň činnosti odborného garanta projektu

Administrátor projektu, projektový manažer je zodpovědný za administraci projektu a to od fáze podání žádosti až po ukončení projektu.(po uplynutí předepsané doby udržitelnosti projektu). Osoba v této roli je dále zodpovědná za sledování plnění úkolů na úrovni vedení projektu, kompletní vedení procesní dokumentace projektu včetně předkládání požadovaných zpráv kontrolním orgánům. Mezi jeho základní požadované dovednosti pro výkon této role patří zkušenosti s administrací větších projektů financovaných ze Strukturálních fondů EU.

Náplň činnosti:

Přípravná fáze	Investiční fáze	Provozní fáze
• Spolupráce při zpracování studie proveditelnosti • Příprava a podání žádosti o poskytnutí dotace, včetně dodání potřebných podkladů a příloh • Spolupráce při vypořádání připomínek (v rámci kontroly přijatelnosti a formální správnosti) • Zajištění potřebných podkladů k podpisu smlouvy o poskytnutí dotace	• Příprava, zpracování a předkládání oznámení o změnách v projektu a podkladů k nim • Administrace projektu, tj. příprava a předkládání monitorovacích průběžných, etapových, závěrečných zpráv a žádostí o platbu a požadovaných příloh • Účast při interních kontrolách, zajištění podkladů pro kontrolu, zajištění součinnosti dalších osob relevantních ke kontrole	• Kontrola zajištění technologických parametrů díla minimálně po dobu udržitelnosti projektu • Příprava a předkládání zpráv o udržitelnosti projektu, monitorovacích zpráv

Tabulka 13 Náplň činnosti administrátora projektu, projektového manažera

Konzultant je osobou v poradenském vztahu vůči zadavateli projektu. Její hlavní úloha je pomoci projektovému týmu a administrátorovi projektu v přípravě žádosti o dotaci a v přípravě podkladů, příloh této žádosti. Dalším jejím úkolem je komunikace se zprostředkujícím subjektem CRR při přípravě žádosti o podporu.

Náplň činnosti:

Přípravná fáze	Investiční fáze	Provozní fáze
• Kontrola formální stránky studie proveditelnosti • Příprava a podání žádosti o poskytnutí dotace, včetně dodání potřebných podkladů a příloh • Spolupráce při vypořádání připomínek (v rámci kontroly přijatelnosti a formální správnosti) • Komunikace s CRR	•	•

Tabulka 14 Náplň činnosti konzultanta

Finanční manažer projektu zajišťuje ekonomickou část spojenou s realizací projektu. Zastupuje tak zadavatele a realizátora projektu ve finanční oblasti v souladu s požadavky programu IROP. Dále je zodpovědný za archivaci účetních dokladů v souladu s pravidly programu IROP, přípravu podkladů pro ekonomické a finanční ukazatele, podklady pro žádosti o platbu, provádění kontroly a archivaci výkazů a aktivní spolupráce v případě kontroly hospodaření projektu. Osoba v roli finančního manažera projektu musí mít znalosti vedení účetnictví dle platných právních norem a zkušenosti s vedením ekonomické části u jiných projektů financovaných ze strukturálních fondů EU.

Náplň činnosti:

Přípravná fáze	Investiční fáze	Provozní fáze
• Odborná konzultace v průběhu zpracování Studie proveditelnosti a žádosti o finanční podporu	• Dohled nad vedením účetní evidence projektu, dohled nad projektem z ekonomického hlediska	• Dohled nad udržitelností projektu z ekonomického hlediska • Příprava ekonomických podkladů k monitorovacím zprávám o udržitelnosti projektu

Tabulka 15 Náplň činnosti finančního manažera

Právník projektu je osobou, která bude v průběhu přípravy a realizace projektu poskytovat odborné konzultace v oblasti právních služeb, a to zejména v případě veřejných zakázek či problémů vzniklých v investiční fázi projektu. Nutným předpokladem pro výkon této role jsou znalosti z oblasti práva, právní problematiky veřejných zakázek a zkušenosti z realizace obdobných projektů.

Náplň činnosti:

Přípravná fáze	Investiční fáze	Provozní fáze
• Odborná konzultace realizovaných výběrových řízení v průběhu přípravy zadávacích dokumentací dle zákona o veřejných zakázkách • Odborná konzultace návrhu plánovaných výběrových řízení v rámci investiční fáze projektu	• Odborná konzultace realizovaných výběrových řízení v průběhu investiční fáze • Konzultace problémů v průběhu investiční fáze z odborné oblasti • Uzavírání smluv, kontrola jejich dodržování	• Konzultace a kontrola dodržování smluv s dodavateli

Tabulka 16 Náplň činnosti právníka projektu

7.2. Popis projektového týmu podílejícího se na přípravě a realizaci projektu v jednotlivých fázích (přípravné, realizační, provozní)

Fáze přípravy projektu

V této fázi projektový tým shromažďuje a zajišťuje veškeré podklady potřebné k podání žádosti, vyhotovuje projektové dokumentace a podává samotnou žádost o poskytnutí finanční pomoci.

Projektový tým v přípravné fázi disponuje kvalitním personálním obsazením a zázemím, nutným k vytvoření koncepce a definice zásadních otázek zajišťujících zdárnou činnost spojenou s přípravou projektu. Součástí přípravy je též konzultace s administrátory dotačních programů, jakožto s realizátory vypracovávající Studii proveditelnosti a další projektové dokumentace. Koordinuje také jednání se zainteresovanými subjekty a potencionálními partnery projektu.

Případné spory řeší v rámci jednání projektového týmu vždy osoba na pozici vedoucího projektu, která určuje zodpovědné osoby, mající za úkol vyřešit spor do určitého termínu. Veškerá komunikace je vedena písemně z důvodu bezproblémového a průkazného předávání informací.

Fáze realizace, provozní fáze

V průběhu fází realizační a provozní disponuje provozní tým kvalifikovaným personálním obsazením, tým rozhoduje v podstatných otázkách ohledně projektu, konzultuje předmět projektu a činnost těchto fází s pracovníky administrujícími dané dotační programy. Dále zajišťuje všechny činnosti spojené s realizací projektu a s průběhy výběrových řízení. Je zodpovědný za řádnou a včasnou realizaci projektu, včetně hlášení o pokroku, průběžných zprávách, zprávách jako podkladu pro financování projektu, monitorovacích zprávách, žádosti o platbu a závěrečné zprávy.

Dodavatel projektu zodpovídá za řádnou a hospodárnou realizaci dodávky, práce dle zpracované projektové dokumentace, platných technických standardů a norem, a dále platné legislativy ČR i EU. Dodavatel by v průběhu prací měl postupovat tak, aby nedošlo k narušení životního prostředí, nejlépe v dobré praxi udržitelného rozvoje. Při jeho pracích by nemělo dojít k poškození stávajícího ani nově pořizovaného vybavení, měl by chránit jako svůj, tak personál zadavatele v bezpečnosti a ochraně zdraví. Řádně vybraný dodavatel musí disponovat řádně kvalifikovanými pracovníky pro zajištění kvalitní dodávky v řádném termínu dle sjednaného harmonogramu. Odbornost pracovních sil dodavatele musí odpovídat požadovaným pracem.

Případné spory řeší v rámci jednání projektového týmu vždy osoba na pozici vedoucího projektu, která určuje zodpovědné osoby, mající za úkol vyřešit spor do určitého termínu. Veškerá komunikace je vedena písemně z důvodu bezproblémového a průkazného předávání informací. Projektový tým se schází pravidelně, jednou za dva týdny. Jsou provedeny zápisy z jednání a ty jsou po potvrzení závazné pro obě strany. Písemně se řeší i veškeré realizační schůzky, které tak upřesňují projektovou dokumentaci nebo definují její změnu.

Interní komunikace zadavatele probíhá formou průběžných porad, svolávaných dle potřebnosti a v závislosti na harmonogramu realizace projektu. Komunikace s dodavatelem nikdy neprobíhá bez přítomnosti nebo vědomí vedoucího projektového týmu.

Požadavky na celkovou kvalifikace projektového týmu

Požadavky na projektový tým zajišťující všechny fáze projektu jsou s vzhledem k rozsahu projektu a jeho cílů a výstupů vysoké. Vysoká odbornost a znalost všech členů týmu včetně předpokládané aktualizace znalostí v průběhu udržitelnosti odpovídá nárokům kladeným tímto projektem. Tyto nároky lze shrnout na tyto činnosti:

- projektové řízení,
- komplexní návrh architektury technického řešení,
- administrace dotace,
- organizace veřejných zakázek,
- finanční řízení projektu;
- komplexní správa technického řešení (včetně pořízeného HW);
- podpora a školení uživatelů;
- ošetření projektu z pohledu legislativy.

Projektový tým, bude v průběhu realizace projektu tvořen na jedné straně zkušenými zaměstnanci KÚ Pardubického kraje a na druhé straně odbornými pracovníky dodavatele. Hlavní roli v řízení projektu bude mít projektový manažer, který bude odpovědný za přípravu a realizaci projektu a jeho rolí je i komunikace s poskytovatelem finanční podpory. Dále bude projektový tým tvořen jedním, nebo více odbornými mentory

odpovědnými za naplnění cílů projektu a výkonnými členy týmu.

8. Řešení projektu

Cílem zvoleného řešení je zajištění vysoké bezpečnosti dat v libovolném časovém okamžiku.
Navrhované řešení sestává z několika komponent, které jsou buď nové, nebo nahrazují stávající nevyhovující řešení. Cílem jejich implementace je zvýšení úrovně zabezpečení LAN sítě Pardubického kraje a provozovaných služeb, a to na úroveň požadovanou vybranými paragrafy Zákona o kybernetické bezpečnosti a běžnými standardy bezpečnosti. Cílem projektu není uvedení sítě do souladu se všemi paragrafy Zákona o kybernetické bezpečnosti, ale ošetření kritických rizik vyplívajících z povahy provozu a hrozeb. Součástí implementace je i zaškolení budoucích správců technických opatření, ať už v jednotlivých technologiích nebo na konci v bezpečnostním provozu jako celku.

8.1. Podrobný popis řešení jednotlivých technických opatření, které žadatel plánuje realizovat v rámci projektu.

Síť Pardubického kraje je vybudována jako částečně redundantní. [redacted]

[redacted]

Síť Pardubického kraje je doménová síť s autentifikací a autorizací vůči Active Directory. Aplikační část i serverová část pracuje na operačních systémech MS Windows. Infrastruktura sítě běží na aktivních prvcích společnosti Cisco, doplněné některými bezpečnostními prvky dalších vendorů. Odborné znalosti administrátorů a správců jsou soustředěny na tyto oblasti.

8.1.1. Opatření - Provedení GAP analýzy

Metodika provedení GAP analýzy se zakládá na zjišťování stavu bezpečnostních opatření proti požadavkům jednotlivých § návrhu č. 316/2014 sb.. V rámci těchto tematických okruhů bude sledována sada dílčích hledisek významnch pro plný soulad se zněním Zákona o kybernetické bezpečnosti České Republiky 181/2014 Sb., a splnění všech parametrů vyžadovaných prováděcí vyhláškou č. 316/2014 sb.. Popsání stávajícího stavu bude doplněno o nápravná opatření odsouhlasená odpovědnými pracovníky krajského úřadu včetně rozpočtových informací.
Celé vypracování GAP analýzy lze rozdělit do tří základních fází:

- V první fázi proběhne rekognoskace prostředí krajského úřadu, jejímž cílem je získání potřebných informací pro zpracování GAP analýzy. V této fázi probíhá intenzivní spolupráce odpovědných zaměstnanců krajského úřadu s Dodavatelem.
- Ve druhé fázi jsou vytěžená data porovnávána s požadavky ZKB a další platné legislativy a Dodavatel identifikuje a hodnotí zjištěné rozdíly.

- Ve třetí fázi Dodavatel spolu se odpovědnými pracovníky krajského úřadu navrhuje nápravná opatření a jejich konfiguraci

8.1.2. Opatření č. 1 – Implementace správy privilegovaných uživatelů a účtů

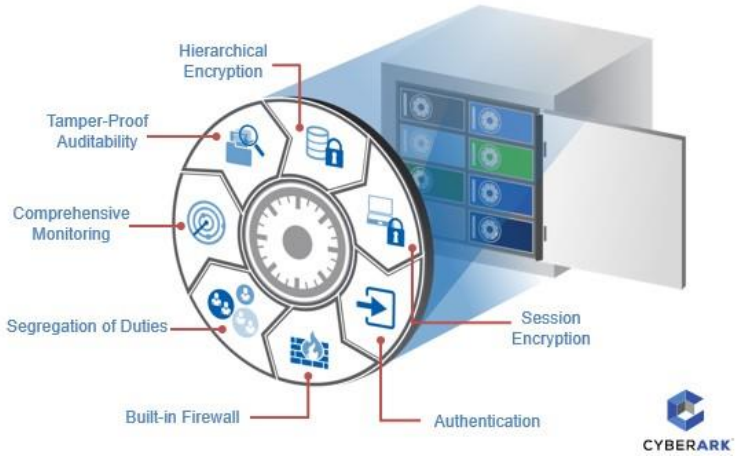
Dané opatření je navřeno s ohledem na zajištění vyšší úrovně IT bezpečnosti, především s ohledem na využívání externích dodavatelů (kdy je nezbytně nutné řídit a monitorovat činnosti a oprávnění externích dodavatelů s vysokými právy /administrátor/, které mohou mít vliv na modifikaci činností jednotlivých IS či jejich částí) a především s ohledem na Zákon o kybernetické bezpečnosti - ustanovení Vyhlášky 316 ze dne 15. prosince 2014 – O bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Součástí opatření jsou navrženy změny

Vaulting Technology®

Architektura privilegovaného zabezpečení účtu je založena na CyberArk's Vaulting technologii. CyberArk zjistil, že oddělením rozhraní serveru ze skladovacího engine, může odstranit mnoho dnešních technologických překážek spojených s bezpečností sítě. Vault technologie vytváří jednotný kanál k přístupu k datům, což výrazně zlepšuje zabezpečení a umožňuje postavit 10 vrstev zabezpečení v jednotném řešení.

Bezpečnostní Vrstvy

Řešení zabezpečení privilegovaných účtů zajišťuje bezpečnost citlivých údajů vaší organizace pomocí mnohonásobných bezpečnostních konceptů, z nichž některé jsou uvedeny stručně níže:



Obrázek 7 - Bezpečnostní vrstvy

- **Hierarchical Encryption** – pro zabezpečení dat v klidovém stavu jedinečným šifrováním každého souboru, trezoru a uložiště. CyberArk také podporuje šifrování serveru úložiště a integruje různé hardware security moduly k zajištění fyzické bezpečnosti serveru
- **Session Encryption** – vestavěná VPN zajišťuje data dovnitř a ven z trezoru během přenosu. To pomáhá chránit proti útokům pomocí odposlechu a je zcela neviditelná pro uživatele
- **Authentication** – zajišťuje identitu uživatele pokoušející se o přístup do systému. CyberArk podporuje různé autentizační metody a integruje přední řešení pro dvoufaktorovou autentizaci
- **Built-in Firewall** – umožňuje pouze provoz, který používá protokol Vault. Tím se snižuje riziko

útoku tím, že brání neoprávněnému, nedůvěryhodnému provoz odkudkoliv v dosažení systému.

- **Segregation of Duties** – umožňuje omezit přístup k úložišti Vault, takže uživatelé mohou vidět pouze svůj jedinečný autorizovaný obsah. Tím se zajistí, že oprávnění uživatelé jsou schopni zobrazit a přistupovat k jejich autorizovaným trezorům, přistupovacím údajům nebo auditních záznamů – ale nic víc
- **Comprehensive Monitoring** – obsahuje monitorování systému pomocí SNMP a integrace s předními dodavateli SIEM a centrálních loggerů pro sledování událostí zabezpečení. Komplexní monitoring pomáhá minimalizovat prostoje, které mohou nechat mezery v ochraně bezpečnosti a upozornění z řešení pomáhají organizacím zjistit podezřelé události dříve, než se stanou vážnými
- **Tamper-proof Auditability** – ukládá auditní záznamy privilegovaných účtů ve vyhrazeném trezoru, a tím zajišťuje, aby oprávnění správci zabezpečení a auditoři byli schopni zobrazit historii aktivity a zároveň zabraňuje uživatelům se zlými úmysly v zakrytí svých kroků

Visual Security

Monitorování v reálném čase, kdo je přihlášen k trezoru a které informace byly získány, umožňuje uživatelům sledovat hesla a soubory v úložišti. Další funkce Visual Security informuje uživatele, kdykoli se vyskytla činnost v trezoru, a označuje hesla a soubory tak, že ty, které byly zobrazeny ostatními uživateli, jsou okamžitě patrné.

Manual Security

Manuální zabezpečení umožňuje uživatelům definovat přístup k trezorům, které obsahují vysoce citlivé informace, takže uživatelé vyžadují manuální potvrzení jednoho nebo více supervizorů trezoru (Safe Supervisors), než budou moci přistupovat k privilegovaným účtům. Oprávnění uživatelé mohou potvrdit požadavky z mobilních zařízení bez ohledu na jejich fyzické umístění, což umožňuje nepřetržité pracovní postupy a prevenci ztráty produktivity.

Geographical Security

The Vault využívá zeměpisná zabezpečení k omezení přihlášení oblastí uživatelů, pouze z určitých oblastí sítě nebo z určitého terminálu.

Ready-to-Use Security

The Vault je plug-and-play, ready-to-use produkt, který realizuje své mechanismy zabezpečení ihned po instalaci. Pracuje s jakoukoliv síťí a neomezeným počtem uživatelů.

Hesla, která jsou uloženy v trezoru, jsou chráněna různými způsoby:

- Heslo - Vault nemůže být otevřen bez hesla a/nebo klíče.
- Časové omezení
- Chráněné oblasti sítě - můžete určit umístění v síti, ze kterých Vault je přístupný.
- Řízení přístupu - můžete definovat úroveň přístup k trezoru pro ostatní uživatele.
- Audit - pokaždé, když soubory jsou zpřístupněné pro jakýkoli účel, aktivita je zapsána v protokolu

činnosti Vaultu

- Kontrola verze - CyberArk Vault sleduje verze uložených hesel a souborů. Kromě toho si můžete obnovit hesla a soubory, které byly dříve odstraněny.
- Duální ovládání - uživatelé mohou potřebovat obdržet povolení od ostatních uživatelů k otevření trezoru
- Protokoly o činnosti - CyberArk Vault vede evidenci všech činností, které probíhají uvnitř. Zobrazí se upozornění pokaždé, kdy dojde protiprávní činnosti v trezoru.

Kombinace těchto aktivních opatření zajistí nejsilnější úroveň ochrany pro své privilegované přístupové údaje a auditní záznamy privilegovaných účtů.

SSH Key Manager brání zneužití SSH klíčů, které jsou privilegovanými uživateli a aplikacemi na platformě Unix/Linux často používané k přístupu k privilegovaným účtům. SSH Key Manager zabezpečuje a především rotuje privilegované SSH klíče založené na bezpečnostní politice privilegovaných účtů a řídí a monitoruje přístup k chráněným SSH klíčům. Toto řešení umožňuje organizacím získat kontrolu nad SSH klíči, které poskytují přístup k privilegovaným účtům, ale jsou často ponechány nespravované:

- Bezpečně uchovává a řídí přístup k soukromým SSH klíčů v Digital Vault
- Automaticky rotuje páry SSH klíčů v souladu s organizační politikou
- Podporuje a prosazuje řízení přístupu k autentizaci a správu požadavků na zvýšení privilegií
- Umožňuje přednastavit politiku vydávání a vracení SSH klíčů
- Umožňuje správcům sledovat a hlásit použití SSH klíčů uživateli a aplikacemi

Enterprise Password Vault / SSH Key Manager podporuje následující funkce:

- ***Možnosti změny hesla***
  - Změna hesla najednou pro jednotlivé osoby/skupiny/všechny systémy založená na zadaných kritériích
  - Změna jednotlivých hesel nebo skupin hesel
    - Automaticky pomocí CPM na základě politiky (každých X dnů nebo na vyžádání)
    - Automaticky pomocí CPM, když heslo není synchronizováno
    - Ručně uživatelem (účet není řízen pomocí CyberArk - pouze uložen)
  - Parametry hesla:
    - Složitost hesla - délka hesla, podpora různých znakových sad, zahrnutí či vyloučení zvláštních znaků
    - Periodicita změn hesla
    - Maximální stáří hesla
    - Unikátní hesla za X posledních změn, podle zařízení

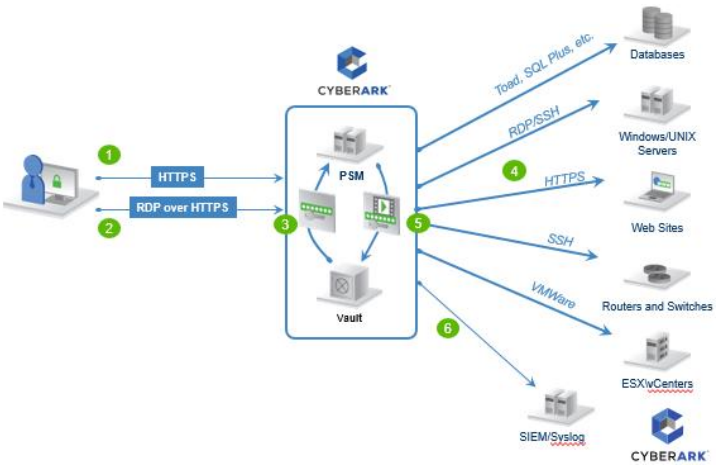
- ***Přístup pomocí hesla***
    - Plné zobrazení - uživatel může přistupovat k privilegovanému účtu a zobrazit heslo bez omezení
    - Bez zobrazení ale s přístupem - uživatel může přistupovat k privilegovanému účtu, ale bez zobrazení hesla
    - Dual control - přístup k privilegovanému účtu nebo zobrazení hesla až po schválení na základě definovaných workflow
    - Omezené
    - Bez přístupu - uživatel nemá možnost zkontrolovat heslo nebo vidět/používat privilegovaný účet
    - Exkluzivní přístup - privilegovaný účet může být využíván pouze jednou osobou v daném okamžiku
    - Jednorázové heslo - po použití privilegovaného účtu, bude změněno heslo
- ***Historie hesla***
    - Historie hesel je uložena po definovanou dobu nebo X posledních změn a může být obnovena ze zálohy
- ***Ověření hesla***
    - Kontroluje, zda heslo uložené v trezoru a na cílovém systému jsou identická
    - Pravidelné kontroly, zda jsou hesla synchronizované - např. každých X dnů
    - Pokud heslo pro spravovaný účet je nesynchronizované, systém informuje e-mailem majitele účtu, aby změnil heslo ručně
    - Nebo lze nastavit, aby se heslo změnilo automaticky pomocí CPM

Enterprise Password Vault obsahuje následující moduly:

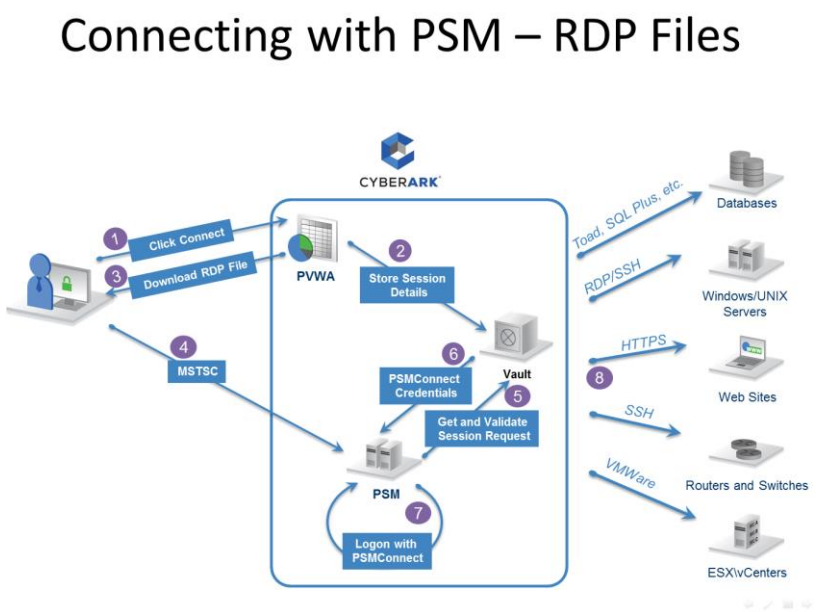
- CyberArk portál, známý jako **Password Vault Web Access (PVWA)**, je jednotný vícejazykový webový přístupový bod pro správu a definování politik pro sdílené a aplikační účty. Umožňuje vyhledávat nahrané relace a nastavit sady root oprávnění k provádění určitých příkazů na vyžádání. Portál je také přístupný z mobilních telefonů, aby bylo možné bezpečně získat přístupové údaje nebo žádat/schvalovat použití privilegovaných přístupových údajů. Password Vault Web Access je přístupný pomocí standardního webového prohlížeče (Microsoft Internet Explorer) a po úspěšném ověření a na základě přístupových práv budou mít IT-Administrátoři přístup k heslům uložených v CyberArk Secure Digital Vault. PVWA podporuje následující metody ověřování: heslo, Windows, Radius, PKI, LDAP, Oracle SSO, a další servery ověřování třetích stran, které lze snadno integrovat. Velmi častým způsobem k ověření CyberArk Secure Digital Vault je použití "ověřování LDAP na základě firemního Microsoft Active Directory", kde uživatelé poskytují své osobní přístupové údaje systému Windows k přihlášení na webové stránky pro přístup k datům uloženým v CyberArk Secure Digital Vault.

- **Central Policy Manager (CPM)** je engine pro privilegované účty, který automaticky řídí a vynucuje firemní heslo/SSH klíče v místních nebo vzdálených sítích v rámci celé firmy bez lidského zásahu. Služba Policy Manager by měla zpracovat změny hesla na cílovém zařízení, jako jsou Windows servery a klienti (lokální a hesla domény, jakož i služby, naplánované úkoly, atd), Unix servery, databáze, síťové prvky atd. Pro změnu hesla slouží přímo přihlášení prostřednictvím spravovaného účtů nebo se používají přihlašovací účty (není-li přímé přihlášení pro spravovaný účet k dispozici).
- **Secure Digital Vault** je patentovaná technologie, která chrání řízení přístupu a informace o zásadách, ukládá nahrávky relací a informace potřebné pro audity. Bezpečná infrastruktura Cyber-Ark zajišťuje, že s privilegovanými účty a nahrávkami nelze manipulovat během přenosu a po uložení.

Privileged Session Manager® – The Privileged Session Manager (PSM) umožňuje organizacím řídit a monitorovat privilegované přístupy do citlivých systémů a zařízení. PSM poskytuje vynikající záznam relace s přehráváním podobné klasickému videorekordéru a nahrávání textu, stejně jako bezpečný vzdálený přístup k citlivým systémům použitím privilegovaného jednotného přihlášení a bez sdělení přístupových údajů koncovým uživatelům.



Obrázek 8 - Funkcionalita PSM



Obrázek 9 - Vazby PSM na RDP

Funkce CyberArk Privileged Session Manager:

Bezpečnost a audit

- Vysoce bezpečné úložiště s využitím FIPS 140-2 ověřené kryptografie pro ukládání všech kontrolních protokolů a zaznamenané relace
- Proxy architektura vytváří izolované a bezpečné prostředí, na rozdíl od potenciálně zranitelných koncových počítačů, kde malware může narušovat správu nebo privilegované relace
- Centralizovaná kontrola a řízení shody (compliance) prostřednictvím vestavěných auditorských zpráv a samoobslužný přístup pro auditory

Přístup k privilegovaným relacím a workflow

- Prosazuje firemní politiky a pracovní postupy, např duální ovládání pro zahájení relace, odeslání důvodu před integrovaných ticketovacích systémů, řízení dobu trvání relace, atd.
- Bezpečný HTTPS přístup umožňuje místní a vzdálený přístup k spravovaným firemním zařízením, podporu pro Remote-App
- Umožnuje nahrávání relace a monitorování podle firemní politiky a rolí koncového uživatele pro jakýkoli druh privilegovaného účtu. Osobní účty a nespravované privilegované účty mohou být také monitorovány pomocí PSM
- Privilegované jednotného přihlášení pro zahájení relace bez nutnosti vystavit privilegované pověření dodavateli třetích stran
- Podporuje širokou škálu protokolů a klientů pro zahájení privilegovaných sezení, včetně Unix, Linux a síťových zařízení (SSH, Telnet), Windows RDP, Radmin, Remotely Anywhere, AS400,

Mainframes, aplikace založené na webu, databáze, hypervisory a nástroje pro správu virtualizace

- Rozšiřitelné díky Universal konektoru (Universal Connector) pro podporu budoucích požadovaných aplikací

Nahrávky privilegovaných relací

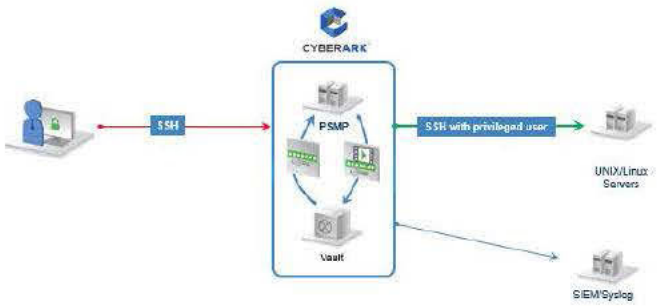
- Přehrávání podobné klasickému videorekordéru zaznamenaných privilegovaných relací pro analýzu událostí a forenzní přezkum
- Textové záznamy SSH relací a audit SQL příkazů v relacích Oracle
- Prohledávat privilegované události s možností vstoupit do záznamu v okamžiku události
- Jeden server podporuje více než 100 souběžných relací záznamů uložených ve vysoce komprimovaném formátu
- Vysoce škálovatelný s možností vyrovnávání zátěže/vysokou dostupností
- Monitorování živé relace
- Ochrana osobních údajů umožňující upozornění na obrazovce uživatele, když je relace záznamenávana

Připravenost enterprise nasazení

- Integrace s CyberArk Shared Technology Platform poskytuje škálovatelnost, vysokou dostupnost a centralizovanou správu a reporting
- Předpřipravená integrace (out-of-the-box) s produkty Privileged Account Security poskytuje kompletní správu, monitoring, nahrávání a bezpečné single-sign-on pro privilegované účty
- Distribuovaná architektura s centrálním řízením a skladování, který je ideální pro prostředí s více sítěmi a lokalit a těží z jednotného rozhraní pro správu, audit a monitoring
- Integrace s firemní infrastrukturou, včetně silného ověřování (dvoufaktorové, SecurID, Radius, PKI, LDAP a další), sledování a SIEM integrace, SNMP, Syslog a SMTP, vestavěný HA / DR architektura a mnohé další

Privileged Session Manager SSH - PSM SSH Proxy (PSMP) zachovává výhody PSM, jako je izolace, kontrola a monitorování, a zároveň umožňuje uživatelům připojit se transparentně na cílové UNIX systémy ze své vlastní pracovní stanici bez přerušení nativních pracovních postupů. PSMP zaznamenává všechny činnosti, které se vyskytují v průběhu privilegovaných sezení v kompaktním formátu ve Vault serveru, kde mohou být přístupné pro autorizované auditory. PSMP je volitelná komponenta, která umožňuje správcům systému UNIX a sítě připojení k privilegovaným účtům, také poskytuje privilegované Single Sign-On funkce, na UNIX zařízení a síťové komponentz transparentně pomocí nativních SSH klientů (jako např putty) aniž by bylo nutné přistupovat k PVWA portálu. Stejně jako u PSM, privilegované relace je připojena skrze proxy a hesla nejsou nikdy sdělovány konečnému uživateli a jejich počítači. Uživatelé mohou získat pouze přístup k účtům, ke kterým mají opravnění a všechny

příkazy jsou zaznamenány ve Vault auditu. PSMP je nasazen na Red Hat Enterprise Linux.



Obrázek 10 - PSM SSH Proxy

8.1.3. Opatření č. 2 - Implementace VPN brány

Stávající VPN brána [redacted] je mimo podporu výrobce. Již se pro tento produkt nevyvíjí žádný nový software [redacted]

Mobilní uživatelé používají verzi VPN klienta [redacted] který nereflektuje plně požadavky nových operačních systému jako je např. Win10 a jeho případné nástupce. Tím je však ohrožen celý vzdálený přístup.

Vzdálený přístup uživatelů úřadu a externích dodavatelů do interní sítě je ukončen na stávajícím [redacted] tyto budou nahrazeny novým systémem. Provoz zařízení s ukončenou podporou výrobce je v rozporu s § 26 vyhlášky 316/2014. Nová VPN brána bude připojena do externí DMZ a bude ukončovat šifrovaný VPN provoz pro mobilní uživatele i pro permanentní IPSec VPN tunely. Hlavním cílem je zajistit v případě potřeby vzdálený přístup pro interní správce i externí dodavatele k informačním i včetně podpůrných systému. Dalším úkolem je umožnění vzdáleného přístupu uživatelům k VIS systémům při plnění jejich běžné agendy. Sekundárně se využijí i pro přístup při práci s ostatními systémy úřadu. Implementace VPN brány zajistí úřadu soulad dle § 17 (šifrování vzdáleného přístupu), § 18 (ověření identity), § 25 (použití vhodných kryptografických prostředků) vyhlášky 316/2014 Implementací web aplikačního firewallu se uvede síť do souladu s § 24 vyhlášky 316/2014.

8.1.4. Opatření č. 3 - Zajištění redundance optických tras pro přístupové switche

Nasazení redundantní optické páteřní sítě jako prostředek pro propojení core a přístupové vrstvy LAN výrazně zlepšuje bezpečnost prostředí a výrazně se podílí na naplnění požadavků ZKB. Instalace záložních tras umožňuje zajistit splnění cílů řízení kontinuity činností a zálohování důležitých technických aktiv informačních a komunikačních systémů včetně významného informačního systému.

8.1.4.1. Vybudování nového přímého propoje datacenter

V suterénu datacenter bude instalováná HDPE chránička 40mm uložena do nově vybudované kabelové trasy. Trasa včetně HDPE chráničky bude ukončena ve stávající kabelové místnosti, kde je vyústěný kabelovod vedoucí z budovy A do budovy C. V budově C kabelovod ukončen v suterénu. Do kabelovodu bude instalována nová HDPE chránička 40mm. Délka HDPE chráničky bude cca 100m. Kabelovod je přístupný z několika míst Komenského náměstí a HDPE trubka lze do tohoto kabelovodu zatáhnout bez stavebních úprav. V datovém rozvaděči budou instalovány 2

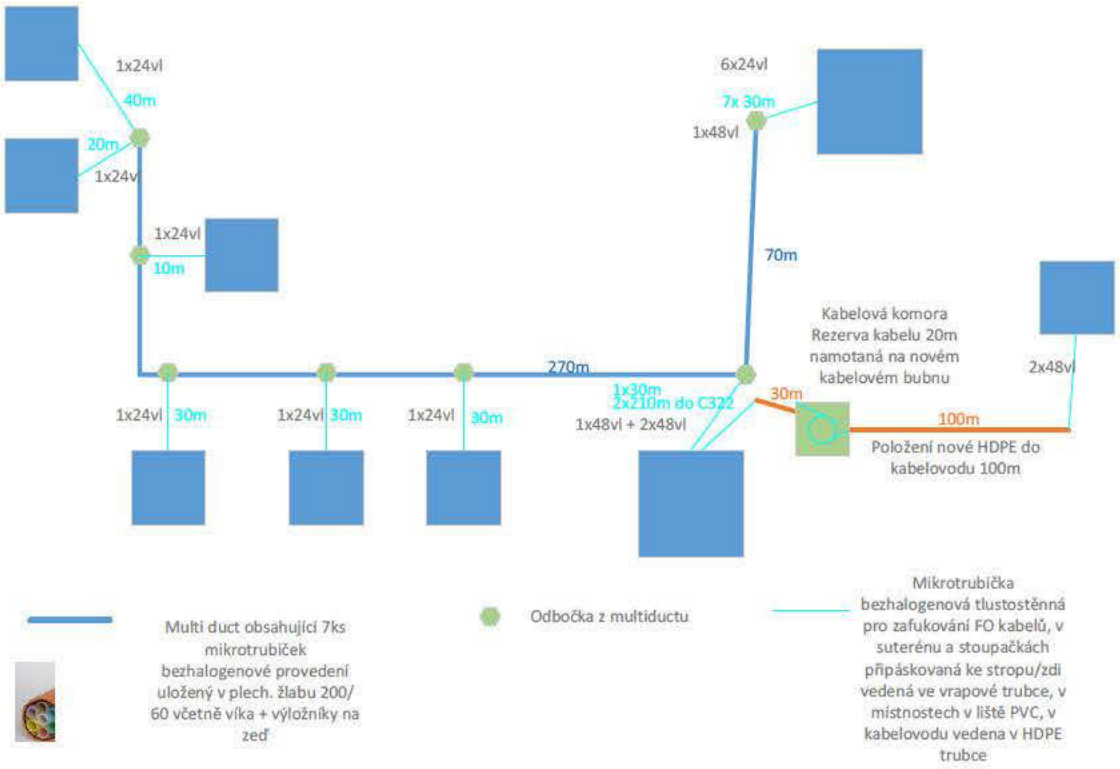
optické vany pro ukončení 48vláken SM 9/125 na SC konektorech PC lomení. Z každé z optických van bude přes průchodku PG natažena nehořlavá (LSHF ochrana) tlustostěná mikrotrubička o rozměru 12/8mm. Trubičky povedou průrazem do suterénu, následně nově vybudovanou HDPE trasou přes kabelovou komoru. V kabelové komoře či dle zadání zadavatele bude instalován nový buben pro uložení kabelové rezervy 20m. Mikrotrubičky povedou přes tento kabelový buben (namotaná rezerva 20m) do HDPE chráničky. HDPE chráničkou do suterénu budovy C a stávajícím stoupacím vedením do místnosti datacentra, kde budou ústit v nově osazených optických vanách stejného provedení jako v protější budově.

HDPE v kabelovodu bude zaplněna mikrotrubičkami plně, aby se předešlo pozdější manipulaci. V místech, kde mikrotrubičky nepovedou v HDPE chráníčce budou zataženy do nově instalované vrapové trubky průměr 40mm. Do obou mikrotrubiček bude zafouknut optický kabel 9/125 48 vláken specifikace ITU g. 657. Bude vytvořena kabelová rezerva 20m. Na obou stranách bude kabel ukončen na pigtailech na SC konektorech formou svařování optických vláken. Optické propoje budou proměřeny certifikačním měřícím přístrojem útlumovou i OTDR metodou a na každé vlákno bude vystaven měřící protokol. Na kabeláž bude poskytnuta záruka v délce min. 20let garantovaná výrobcem.

8.1.4.2. Vybudování redundantní optické páteřní sítě sekundárního datacentra a posílení propoje datacenter budovy A

V suterénu za datacentrem bude instalována nová kabelová trasa z plechového žlabu o rozměru min. 200/60mm. Součástí kabelové trasy bude víko a výložníky, pomocí kterých bude kabelová trasa přichycena ke zdi. Trasa povede suterénem do budovy B, kde bude končit pod nejvzdálenější z rozvaděčových místností. Do kabelové trasy bude instalován nehořlavý multiduct (LSHF ochrana) jehož součástí je 7ks mikrotrubiček o rozměru 10/8. V místech odbočky k příslušnému podružnému rozvaděči bude z Multiductu vyvedena přes redukční spojku tlustostěnná nehořlavá mikrotrubička o rozměru 12/8mm. Trubička povede vrapovou trubkou do stoupačky a následně do příslušné místnosti s podružným rozvaděčem, kde bude mikrotrubička přes průchodku PG ukončena v optické vaně v datovém rozvaděči. V některých případech bude trubička vedena k datové místnosti stoupacím vedením PVC lištou. Na straně datacentra bude napojeno na multiduct 7ks mikrotrubiček a vrapovými trubkami budou protaženy do datového rozvaděče, kde budou ukončeny v optických vanách. Do mikrotrubiček vedoucích do podružných rozvaděčů bude zafouknut optický 24vláknový mikrokabel SM 9/125 specifikace ITU g. 657. Do mikrotrubičky propojující datacentra budovy A bude zafouknut kabel 48vl. SM 9/125 ITU g. 657. V místnosti datacentra bude vytvořena ve dvojité podlaze kabelová rezerva 20m na všech kabelech. Na obou stranách budou kabely ukončeny na pigtailech na SC konektorech formou svařování optických vláken. Optické propoje budou proměřeny certifikačním měřícím přístrojem útlumovou i OTDR metodou a bude na každé vlákno vystaven měřící protokol. Na kabeláž bude poskytnuta záruka v délce min. 20let garantovaná výrobcem.

Topologie navrženého řešení:



Obrázek 11 - Topologie navrženého řešení

8.1.5. Opatření č. 4 – Doplnění přístupových přepínačů

Hlavními cíly opatření je zajištění náhrady zastaralých a výrobcem nepodporovaných přístupových [redacted] přepínačů. Je zde snahou zajistit co nevyšší dostupnost VIS při případných pokusech zneužití bezpečnostních zranitelností přepínačů. A to dle §26 (Nástroje pro zajištění vysoké úrovně dostupnosti) prováděcí vyhlášky zákona 316/2014 Sb. Obdobnou problematiku řeší vytvoření redundantních datových spojů mezi přístupovými a páteřními přepínači.

Dále je snahou zajistit identickou bezpečnostní politiku skrz celou síťovou infrastrukturu. Využít, technicky a odborně pak rozšířit stávající bezpečnosti řešené pomocí IEEE 802.1x přes celou síť a to z pohledu autentizace a autorizace při přístupu do LAN,. včetně přiřazování příslušných VLAN uživately/zařízení a tím řídit integritu sítě. Zde dojde k naplnění §17 (Nástroj pro ochranu integrity komunikačních sítí), §18 (Nástroj pro ověřování identity uživatelů), §19 (Nástroj pro řízení přístupových oprávnění), prováděcí vyhlášky zákona 316/2014 Sb.

Při aplikaci zasílání informací o datovém provozu do centrálních NetFlow kolektorů a jeho vyhodnocení z pohledu KBU dojde k realizaci §22 (Nástroj pro detekci kybernetických bezpečnostních událostí) prováděcí vyhlášky zákona 316/2014 Sb.

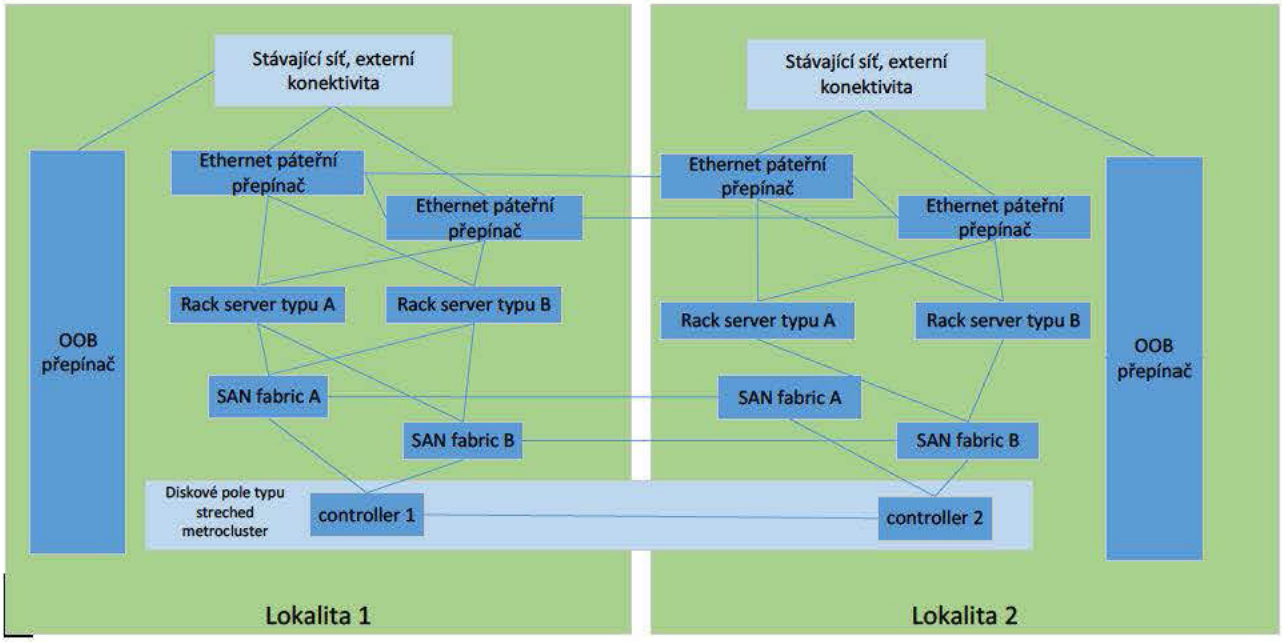
Obměna přepínačů na pronajmutém optickém datovém spoji mezi centrální lokalitou a spisovnou, které budou veškerou komunikaci šifrovat pomocí technologie MAC SEC, zajistí v této části sítě soulad §17 (Nástroj pro ochranu integrity komunikačních sítí) a §25 (Kryptografické prostředky) prováděcí vyhlášky zákona 316/2014 Sb.

8.1.6. Opatření č. 5 - Doplnění HW Datového centra o servery a pole

Stávající propojení lokalit pomocí FC je realizováno pomocí 8G FC na stávajících přepínačích. Tato propustnost nemusí být dostatečná pro zvolenou variantu v případě výpadku řídícího kontroléru na diskovém systému v jedné lokalitě. Zároveň lze identifikovat nedostatek volných portů na stávajících SAN přepínačích.

Pro splnění požadavků §26 - Nástroj pro zajišťování úrovně dostupnosti je třeba doplnit HW a SW datového centra tak, aby byl vytvořen vysoce dostupný systém, který bude spolu se stávající infrastrukturou poskytovat služby v odpovídající kvalitě a především se zaručenou dostupností.

Navržené řešení je postaveno na technologii Stretched metroclusteru využívajícího pro svoji komunikaci FC SAN síť.



Obrázek 12 - Topologie navrženého řešení DC

Konkrétní řešení je postaveno na technologii Netapp doplněné síťovou infrastrukturou a výpočetními prostředky postavenými na prvcích Cisco Systems. Takto navržené řešení umožní oddělení frontend a backend provozu ve formě dvou nezávislých sítí LAN a SAN a u přináší možnost komunikace se stávajícím řešením využívajícím stejnou architekturu oddělené LAN a SAN bez výrazné rekonfigurace. Řešení diskového systému zajišťuje jednak diskovou kapacitu a zároveň aplikačně konzistentní backup

Servery pro zajištění dostatečného výpočetního výkonu jsou dvojího typu. Server typu A je určen pro aplikace, které nemohou být virtualizovány nebo z bezpečnostního důvodu není vhodné, aby využívali sdílený výpočetní výkon. Tyto servery proto běží v režimu bare metal. Na tyto servery je přímo instalován operační systém Microsoft Windows Server 2016 standard. Servery typu B jsou virtualizovány. Současné řešení je postaveno na technologii společnosti [redacted] a již obsahuje centrální management software virtuální infrastruktury [redacted] Pro zajištění kompatibility stávajícího a nového prostředí, zajištění maximálního využití výpočetního výkonu a možnosti přenášet virtuální servery ze stávající do nové infrastruktury, je požadováno, aby servery typu B byly virtualizovány pomocí řešení [redacted] standard společnosti [redacted] Všechny tyto servery budou zařazeny pod společný, již existující, [redacted] Pro zajištění vysoké dostupnosti jsou tři servery typu A a dva servery typu B v lokalitě 1 a zároveň dva servery typu A a jeden server typu B v lokalitě 2.

Technicky se u všech serverů jedná o vyšší kvalitativní třídu s možností vzdáleného přístupu a vzdáleného ovládání provozu na daných serverech přes dedikovaná fyzická rozhraní.

8.1.7. Opatření č. 6 – Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě

V současnosti [redacted] Lokální síť je dostupná nejen v centrální lokalitě, ale i několika dalších pobočkách či úřadem zřízených institucích. Administrátoři se při přístupu k síťovým prvkům ověřují [redacted]
Aktuálně je v sítí úřadu nasazována ochrana proti neoprávněnému přístupu pomocí technologie 802.1x. V síti se nacházejí i zařízení, [redacted] Každý administrátor, který má oprávnění přistupovat a měnit konfiguraci na Cisco ISE, může registrovat MAC adresy do Cisco ISE bez časového omezení a důvodu. Navrhovaná aplikace, MABKeeper má za úkol vytvořit centrální databázi MAC adres zařízení, které se mohou v síti ověřovat a zajistit, aby pouze oprávněný a auditovaný administrátor mohl databázi modifikovat a svůj postup zdůvodnil. Aplikace OfficeLocator následně zajišťuje centrální monitoring koncových portů, které jsou ověřovány pomocí protokolu 802.1x.

Nově implementovaný systém zajistí další možnosti řízení přístupu do LAN i WiFi sítě a to nejen pro úřadem vlastněné stanice, ale i mobilní zařízení. Systém je schopen zajistit ověřování uživatelů (úředníků) v centrální databázi identit, ale i tzv. hostů, návštěvníků úřadu pro přístup do sítě Internet.
Systém bude implementován v podobě redundantních AAA serverů, připojených v obou lokalitách do segmentu síťového managementu. Tento segment bude zabezpečen proti neautorizovanému přístupu.
Stávající autentizační systém používaný pro účely správy síťových prvků bude rozšířen na nově implementovanou platformu a umožní i autentizovat, autorizovat a logovat informace o přístupu a činnostech administrátorů, spravujících síťové prvky. S ohledem na §18 vyhlášky 316/2014 bude nastaven tak, aby vynucoval komplexitu hesla pro administrátory, zamezil opakovanému použití starších hesel a vynutil změnu hesla po uplynutí doby definované doby. V souladu s §18 a §21 vyhlášky 316/2014 bude autorizovat jednotlivé administrátory při přístupu na síťové prvky a bude o jejich činnosti sbírat auditní informace. Ty bude přeposílat do centrálních auditních systémů (logmanagenent, management přístupu privilegovaných účtů)
Před povolením přístupu pro dané zařízení ověří ISE systém uživatele a nebo zařízení a podle nastavených politik uživateli umožní např. přístup nebo ho zamítne. Internímu uživateli na úřadem vlastněném zařízení přístup do vnitřní sítě povolí a ostatním umožní pouze přístup do sítě pro hosty, určené pro přístup do sítě Internet. Interní uživatelé budou autentizováni ověřením jejich uživatelských účtů zprostředkovaně doménovým řadičem úřadu a z pohledu implementovaného systému nebudou jejich uživatelské účty spravovány lokálně. Přístup uživatelů do sítě úřadu tak bude uveden do souladu s §18, §19 a §21 vyhlášky 316/2014.
Navrhovaná aplikace využívá API rozhraní, které nabízí Cisco ISE, k možnostem správy databáze MAC adres, které se využívají k ověřování v síti pomocí protokolu 802.1x. Aby byl uživatel schopen komunikace s databází Cisco ISE, musí se do aplikace přihlásit a mít dostatečné oprávnění k zápisu do definované skupiny MAC adres. K tomu slouží integrace aplikace pomocí LDAP konektoru s identity databází. Aplikace kombinuje vlastnosti řízení přístupu pomocí oprávnění definované v externí databázi a komunikuje s Cisco ISE pomocí API rozhraní.

Pro monitoring sítě podléhající 802.1x je další aplikace důležitá v přístupu zpracování údajů. Aplikace je schopna získávat logy generované síťovými přepínači a Cisco ISE, na základě kterých dodává ucelené informace o stavu koncových stanic a uživatelů přihlášených do sítě.

- Zvolené referenční řešení

8.1.7.1. Aplikace MAB Keeper

Aplikace MAB Keeper umožňuje spravovat některá nastavení autentizačního systému bez přímého přístupu do jeho konfiguračního rozhraní. Aplikace díky několika modulům pokrývá různé případy užití, díky nimž je možné řešit problémy, které se typicky mohou vyskytnout po implementaci 802.1x kvůli chybějícím nebo nekompatibilním IT procesům. MAB Keeper obecně slouží pro správu MAC adres zařízení, které se v autentizačním systému používají pro autentizaci zařízení a nejsou kompatibilní se standardem 802.1x (tiskárny, IP telefony aj.) nebo pro správu MAC adres zařízení, u nichž se MAC adresa používá pro autentizaci. Takovým zařízením je vytvořena výjimka pro přístup do sítě díky přidání do autentizačního systému. Ke každé výjimce jsou evidovány různé informace, které usnadní případný troubleshooting nebo rozhodování o dalším prodloužení výjimky.

Mimo pasivních zařízení a zařízení, která se z libovolného důvodu nemohou autentizovat, umožňuje aplikace spravovat a kontrolovat přístup zařízení, u nichž je MAC adresa využita jako náhradní způsob autentizace. Typicky se jedná o zařízení konzultantů, která potřebují po určitou dobu přístup do firemní sítě, nebo o BYOD zařízení zaměstnanců. U takových výjimek je navíc evidován Sponsor, který připojení zařízení do sítě schválil a nese příslušnou odpovědnost. Speciálním případem je možnost zablokování přístupu pro určité zařízení, a to buď jako preventivní opatření, nebo v rámci reakce na hrozbu, kterou pro síť již připojené zařízení představuje. V závislosti na účelu může být výjimka časově omezená, taková je po uplynutí stanoveného času z aplikace i autentizačního systému odmazána bez nutného zásahu administrátora.

Nad každou operací, kterou aplikace vykoná automaticky a nad každým úkonem, který vykoná uživatel přes rozhraní aplikace, je veden detailní log. Ten napomůže případnému troubleshootingu či security auditu. Přístup do jednotlivých modulů aplikace je možné řídit na základě definovaných rolí uživatelů díky jejich členství ve skupinách v Active Directory.

8.1.7.2. Aplikace Office Locator

Aplikace Office Locator představuje helpdeskový portál, který slouží k monitoringu a analýze 802.1x autentizace a poskytuje oprávněnému uživateli informace z různých zdrojů potřebné pro určení příčiny problému s autentizací či řešení incidentu v jednoduchém webovém rozhraní. Aplikace registruje jednotlivé autentizační relace a prezentuje jejich stav spolu s dalšími informacemi z Cisco ISE, Active Directory a síťových přepínačů. Uživatel tak má možnost si například zkontrolovat účet uživatele v Active Directory či konfiguraci portu na přepínači, aniž by měl do těchto systémů přímý přístup. Dostupnost různých funkcionalit je řízena díky členství uživatelů ve skupinách v Active Directory.

Obě aplikace jsou vzájemně integrované a pro některé funkcionality si navzájem poskytují potřebná data.

- možnost výjimky pro přístup do sítě časově omezit a nechat aplikaci automaticky odmazávat

- omezení přístupu do aplikací dle definovaných rolí uživatelů
- odstínění uživatelů od konfiguračního rozhraní Cisco ISE, síťových přepínačů i Active Directory
- možnost customizace aplikací i uživatelského rozhraní pro specifické potřeby zákazníka
- dostupnost informací z různých zdrojů potřebných pro troubleshooting a řešení problémů

8.1.8. Opatření č. 7 – Centrální logovací nástroj

Pro naplnění požadavku zákona, ale i ve smyslu osvědčené bezpečnostní praxe je třeba zajistit službu komplexního řešení pro zaznamenávání aplikačních logů vznikajících na infrastruktuře Pardubického kraje s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných aplikací a ostatních informačních systémů na serverové části včetně možnosti jejich uložení do neměnné databáze.

Pro zajištění dlouhodobé auditní stopy, podporu IT a základní bezpečnostní monitoring je nezbytné zavést řešení na centralizaci a správu logování. Jedná se mimo jiné o naplnění §21 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů, §22 Nástroj pro detekci kybernetických bezpečnostních událostí, §23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

Pro potřeby bezpečnostního monitoringu budou sbírány všechny relevantní informace, které se týkají zejména:

- Přihlašování uživatelů
- Přihlašování privilegovaných účtů (Administrátoři, technické a servisní účty)
- Činnosti uživatelů a administrátorů v rámci aplikace
- Pokusy o neautorizovaný přístup
- Bezpečnostní chyby
- Změny auditní politiky
- Změny oprávnění
- Výstupy z auditních modulů aplikací

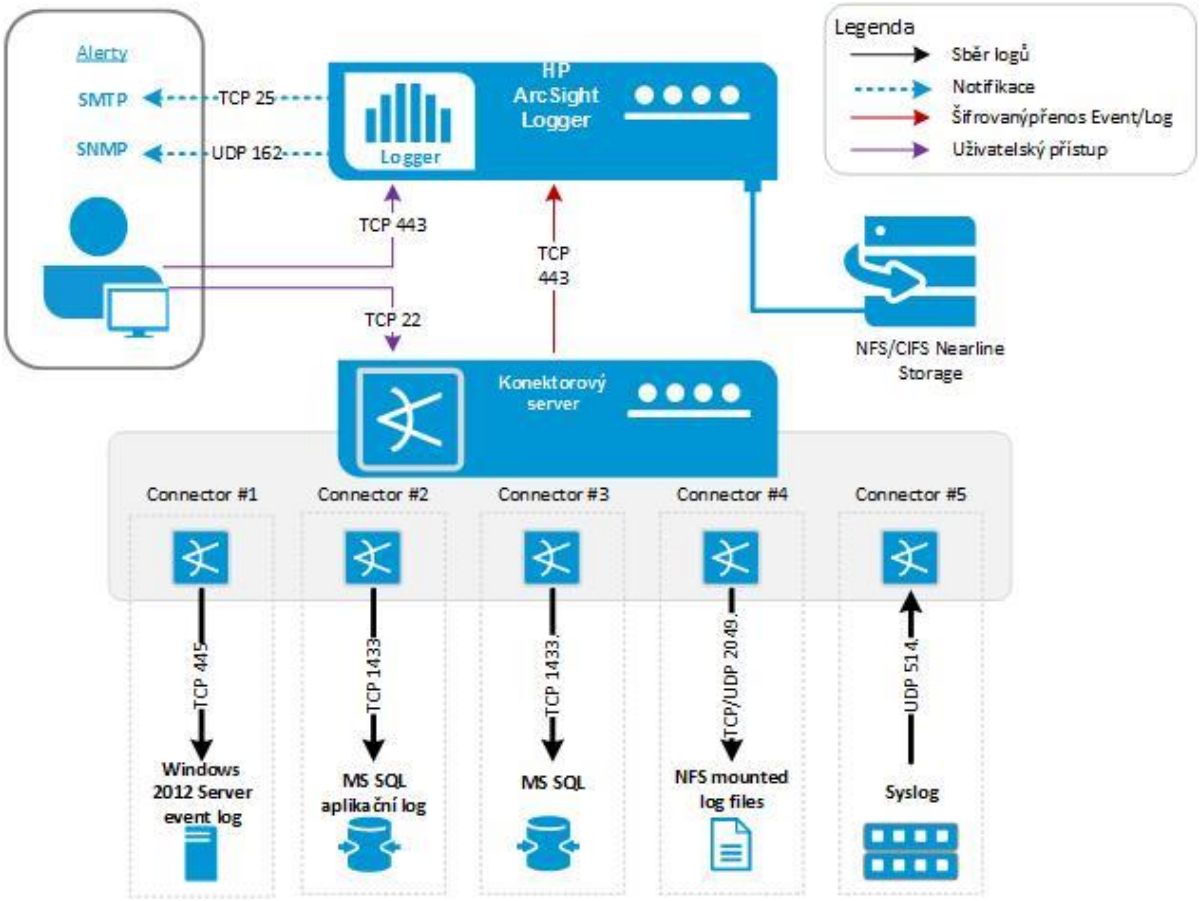
Pro zajištění bezpečnostního dohledu je navrženo technické řešení postavené na technologii HP ArcSight. V rámci bezpečnostního dohledu je realizován sběr logů, které obsahují relevantní informace z pohledu bezpečnosti, budou systém zpracovány do jednotného formátu (CEF), ukládány a vyhodnocovány.

ArcSight Logger podporuje sběr syrových nebo nestrukturovaných záznamů z libovolných systémových nebo souborových protokolů (syslog ap.) a disponuje také obrovskou knihovnou konektorů (ArcSight Connectors), které dokáží sbírat údaje z více než 300 různých zdrojů generujících vlastní protokoly. Kromě toho zahrnuje i nástroj ArcSight FlexConnector, který možnosti sběru dat dále rozšiřuje i na libovolné zákaznické zdroje a firemní aplikace potřebné kvůli regulačním nařízením a forenznímu zkoumání. ArcSight Connectors se dají nasazovat jako software nebo jako speciální zařízení do datových center a do lokálních poboček, aby tam zajistily bezpečný a spolehlivý sběr údajů. Tyto konektory také nabízejí kontrolu šířky pásma, určování priorit pro posílání záznamů,

lokální ukládání a další opatření za účelem minimalizace ztráty dat, resp. nežádoucího ovlivňování kritických podnikových procesů.

HP ArcSight Logger má pro konkrétní role různé personalizované ovládací panely, kterými jsou potřebné výstupy sdruženy do jediné konzole. Z těchto souhrnných ovládacích pultů se pak uživatel snadno dostane i na specifické reporty a simulované auditní postupy. Výkazy (reporty) v HP ArcSight Loggeru dodržují obecný formát pro události a nevyžadují žádnou znalost podoby protokolů pocházejících z jednotlivých zdrojů. Není proto nutné analyzovat záznamy ze specifických zařízení konkrétních výrobců. Zajímavé výsledky obsažené ve výkazech lze dále analyzovat pomocí jednoduchého vyhledávání ve stylu Google, a tak zkoumat libovolná strukturovaná i nestrukturovaná zaznamenaná data. Také je možné definovat vyhledávací šablony, které se v případě shody použijí k okamžitému varování na konzoli ArcSight Loggeru nebo přes SMTP, SMNP ev. syslog. Uživatelé se navíc z obdrženého varování mohou dostat přímo do podkladové databáze událostí, které toto varování vyvolaly, a analyzovat původní příčinu. Právě tady má klíčový význam nestrukturované vyhledávání plus rychlost a výkonnost, protože analýza může vést na data, která jsou buď hodně stará, nebo jsou v jiném formátu. Tento logický průchod různými formami analýzy eliminuje nutnost připravovat si v každé fázi zkoumání nový obsah.

V budoucnosti je možno daný logovací management rozšířit do plnohodnotného systému SIEM pouze povýšením licence a povýšit tak hodnotu investice projektu.



Obrázek 13 - Centrální logovací nástroj

8.1.9. Opatření č. 8 - Implementace vysoké dostupnosti pro [redacted]

Stávající [redacted] databáze VIS GINIS je provozována [redacted] V případě její nedostupnosti je [redacted] Pokud je poškození databáze nebo HW nevratné, tak je nutné provádět obnovu ze zálohy, což znamená minimálně celodenní výpadek.

- Je zde nesoulad s §25 prováděcí vyhlášky zákona 181/2014 Sb.

Stávající implementace [redacted] databáze pro VIS GINIS je pouze jenom v jedné instanci. V případě jejích nedostupnosti nebo poškození vzniká výpadek, který není akceptovatelný z pohledu provozu VIS. Řešením je replikace dat do druhé databáze., která bude provozována na záložním HW. Vytvořením záložního zdroje dat je zkrácena doba případného výpadku na přijatelnou úroveň. Nedostatečně řešená vysoká dostupnost podpůrného aktiva VIS je v rozporu s § 26 (Nástroje pro zajištění vysoké úrovně dostupnosti) prováděcí vyhlášky zákona 316/2014 Sb.

8.1.10. Opatření č. 9 - Implementace řešení pro monitorování toků

V souladu s § 20 a § 22 prováděcí vyhlášky 316/2014 se použije nástroj, který zajistí detekci nestandartního chování uživatelů a aplikací, které komunikují na síťové úrovni. Smyslem je detekce nevhodně se chovajících aplikací a uživatelů a zejména pokročilého malwaru, který by mohl ohrozit privátnost, dostupnost a integritu aplikací Významného informačního systému, dalších informačních a komunikačních systémů.
Vybraným řešením je produkt společnosti Flowmon Networks – Flowmon sondy, Flowmon kolektor. Jedná se o technicky a finančně ideální řešení na monitorování datových toků s možností doinstalování dalších přídavných modulů a tím rozšiřování možností tohoto řešení. Jedním z těchto modulů je i nástroj na behaviorální analýzu chování uživatelů na síti. Je tedy možné sledovat síť nejen z hlediska anomálií, ale i z pohledu provozního monitoringu. Celé řešení pak spolupracuje s centrálními logovacími nástroji. Další nespornou výhodou je podpora ze strany české výrobce. Z cenového hlediska se jedná o velmi výhodnou investici z hlediska visibility sítě vůči kybernetickým hrozbám

8.1.11. 0patření č. 10 – Doplnění redundantní [redacted] proxy

Stávající proxy brána [redacted] je mimo podporu výrobce. Již se pro tento produkt nevyvíjí žádný nový software a nejsou řešeny ani nově objevené zranitelnosti. Je zde tedy riziko kompromitace při objevení nových zranitelností. Navíc nejsou chráněni uživatelé vůči aktuálním bezpečnostním hrozbám, protože absence updatů na nové typy útoků zvyšují riziko kompromitace uživatelských zařízení, které pracují s informacemi.
V případě využití stávající plně podporované proxy brány je zde probém v případě jejího výpadku, kdy jsou k dispozici pouze dva scénáře.

- Nefukční veškeré HTTP/HTTPS aplikace
- Lze pustit provoz do Internetu napřímo, ale za cenu neřízeného a nezabezpečeného přístupu.

Většina uživatelů síti KÚ pracuje s VIS systémy a zároveň přistupuje do internetu. Většina podpůrných aktiv VIS též vyžaduje pro svoji aktualizaci internetovou konektivitu. Provoz do internetu musí být chráněn před škodlivým kódem, který jako jeden z hlavních vektorů pro jeho šíření využívá WWW komunikaci. Tuto ochranu řeší [redacted]

web proxy systém. Web proxy naplňuje §17 a §20 prováděcí vyhlášky 316/2014, kdy dochází k ochraně integrity komunikační sítě a k ochraně před škodlivým kódem. Provoz zařízení s ukončenou podporou výrobce je v rozporu s § 26 vyhlášky 316/2014, protože není zajištěna vysoká dostupnost systému. Proto se navrhuje výměna zastaralé brány, která již neplní dostatečně své bezpečnostní (výrobcem je již nepodporovaná), za nový model plně kompatibilním se stávajícím boxem.

8.1.12. 0patření č. 11 – Rozšíření [redacted] o SANDBOX

Stávající antivirová řešení, která jsou umístěná na [redacted] proxy branách, operačních systémech serverů a uživatelských zařízeních nejsou schopny řešit problematiku „day zero“ útoků a hrozeb. Webový provoz je jedním z nejčastějších vektorů šíření škodlivého kódu. V případě nového typu malware nákazy nedokáží boxy tuto hrozbu detekovat a případně zastavit. Dochází zde k nesplnění §20 prováděcí vyhlášky zákona 181/2014 Sb. Tímto rizikem jsou ohroženy podpůrná aktiva VIS a stanice uživatelů, kteří pracují s aktivy VIS. Provoz běžných antivirových řešení na proxy branách a koncových operačních systémech je nutností. Ale je nutné tyto funkcionality rozšířit o sandbox funkce, které jsou schopny detekovat nové typy malwaru, na které nejsou konvenční antivirová řešení schopny dostatečně rychle zareagovat

8.1.13. Opatření č. 12 - Implementace Webového aplikačního firewallu

V souladu s § 22, § 24 a § 26 prováděcí vyhlášky 316/2014 vznikne ochrana perimetru před aplikačními DoS útoky a vznikne infrastruktura zajišťující vysokou dostupnost elektronických služeb poskytovaných krajským úřadem.

Vložením vhodné technologie z pohledu kybernetické bezpečnosti přinese:

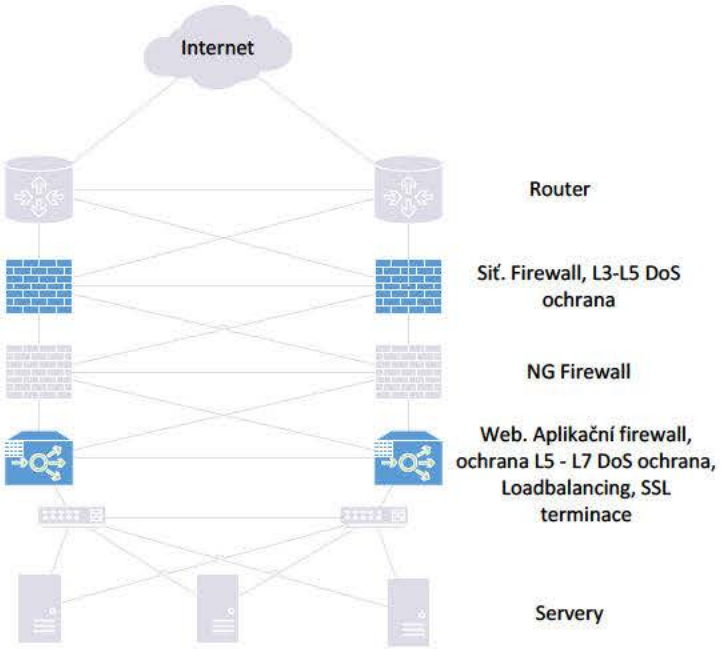
- Plnou náhradu funkcionality stávajícího [redacted]
- Autonomní vrstvu inspekce webového provozu
- SSL offload (SSL terminace) a inspekce provozu
- Logování a korelace bezpečnostních událostí
- Potlačení aplikačních DoS (DDoS) útoků

V nově vytvořené DMZ vznikne vrstva ochrany před aplikačními DoS útoky.

8.1.13.1. Řešení F5 BIG-IP

Pro zajištění ochrany před aplikačními DoS útoky byla vybrána technologie F5 BIG-IP, která splňuje všechna hlediska specifikovaná v textu výše. Řešení předpokládá vznik vrstvy abstrakce mezi klientem a serverem, realizováná ochrana webových aplikací, monitoring a vysoká dostupnost aplikací a ochrana před aplikačními (web) DoS útoky.

Obě vrstvy jsou znázorněny modře v následujícím obrázku.



Obrázek 14 - Topologie navrženého řešení WAF

8.1.13.2. Webový aplikační firewall a ochrana před L5-L7 DoS útoky

Tento dedikovaný firewall F5 BIG-IP ASM (Advanced Security Manager) pracující na aplikační úrovni ISO OSI modelu bude poskytovat ochranu webových aplikací před kybernetickými útoky využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách, tj. explicitní povolení legitimního provozu (pozitivní logika) a zakázáním provozu, který je známý kybernetický útok. Zejména vhodné nastavení pozitivní logiky dokáže chránit webovou aplikaci proti tzv. Zero Day útokům. Webový aplikační firewall také bude poskytovat ochranu proti aplikačním DoS útokům zaměřených na webové aplikace. Součástí webového aplikačního firewallu bude také licence pro load balancer F5 BIG-IP LTM (Local Traffic Manager), který bude zajišťovat monitorování dostupnosti poskytovaných služeb, provádět SSL terminaci, rozkládat nutnou aplikační zátěž mezi jednotlivé aplikační/webové servery.

Webový aplikační firewall tedy přinese komplexní zabezpečení webových aplikací, především pak:

- Ochrana proti aplikačním DoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky apod.)
- Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, manipulace s cookies, ochrana parametrů, URL apod.
- Session Management – ochrana proti únosům relací
- Brute Force Ochrana – ochrana před prolomení hrubou silou
- SSL terminaci
- Monitorování dostupnosti služeb
- Vysokou dostupnost služeb

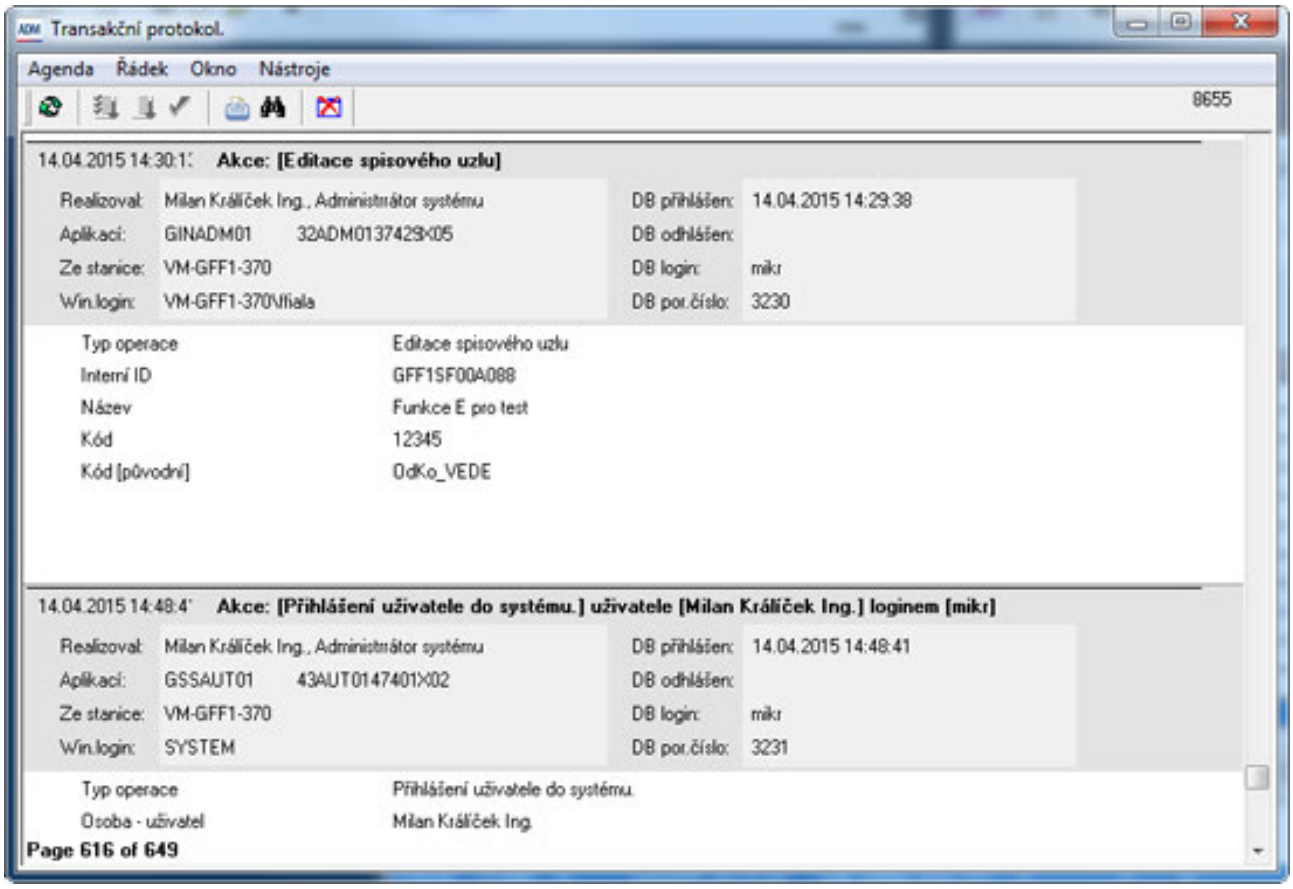
- Rozklad aplikační zátěže

8.1.14. 0patření č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS

V rámci standardní instalace systému GINIS nedochází ke sběru transakčních logů z jednotlivých modulů systému tak, jak je to vyžadováno § 21 prováděcí vyhlášky 316/2014. Stávající moduly systému GINIS tak nejsou ani schopny bez navrhovaného rozšíření předávat logy do centrálního logovacího nástroje nebo SIEMu. Stávající systém umožňuje neoprávněnou manipulaci s logy.

Pro zajištění souladu s požadavky zákona proto bylo navrženo pořízení modulu „Transakční protokol" dodávaného vývojáři tohoto integrovaného systému systému. Jeho implementace zajistí plnění všech požadavků zákona a výrazně tak zvyšuje bezpečnost systému GINIS. Transakční protokol představuje rozšíření modulu Základní administrace – po jeho aktivaci jsou v systému sledovány a zaznamenávány změny dat administrace. Sledovány jsou dvě skupiny dat, klíčová a ostatní.

U klíčových dat, která mají zásadní vliv na přihlášení uživatele, se sledují realizované změny v datech, a to včetně měněných hodnot. Je tak např. zaznamenán jak původní login osoby, tak nově nastavený login. Do této skupiny dat patří např. osoby, přihlašovací účty, role, parametry aplikací. U všech ostatních dat administrace se zaznamenávají již pouze události spojené se záznamem (např. záznam byl založen, editován, zobrazen).



Obrázek 15 - GINIS - Transakční protokol

Dále jsou podrobně sledovány události a jejich data spojená s přihlášením uživatelů, jakou jsou úspěšné přihlášení uživatele do GINISu, neoprávněný pokus o přihlášení (uživatel neměl oprávnění přístupu) nebo neúspěšný pokus o přihlášení přihlašovacím účtem do databáze. Výčet sledovaných oblastí lze nastavit v rámci administrace.

Transakční protokol je v rámci systému GINIS přístupný pouze pro čtení, editace není možná. Jeho obsah lze zobrazit v rámci Základní administrace nebo protokol generovat do formátu PDF nebo XML.
Transakční protokol bude následně napojen na systém sběru událostí (opatření č. 9), události systému GINIS lze také v budoucnu průběžně odesílat do externího SIEM systému který výrazně rozšiřuje monitoring.

8.1.15. 0patření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů

Přenos dat mezi aplikací GINIS a datovým uložištěm aktuálně probíhá [redacted] Toto řešení je v rozporu s požadavky zákona a nemůže být nadále úřadem využíváno. Navíc úřadem využívané úložiště [redacted] má rezervy v kapacitě, a proto je vhodné použít řešení na bázi napojení významného informačního systému GINIS konektorem do datového úložiště [redacted]

8.1.16. 0patření č. 15 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů

Správná identifikace uživatelů a administrátorů při přístupu do počítače nebo k aplikacím / službám je zcela zásadní otázkou v rámci informační bezpečnosti. Jsme-li schopni jednoznačně identifikovat jména uložená v logách operačních systémů a aplikací, můžeme prostřednictvím auditu zjistit, co dané osoby dělaly. Nejjednodušším příkladem identifikátoru je jméno nebo název účtu a příslušné heslo. Toto je ale v současné době zejména pro administrátory, ale i pro osoby mající přístup k významným informačních systémů, považováno již za nedostatečné. Kombinace uživatelského jména a hesla s některou z dalších metod ověření výrazně snižuje riziko zneužití účtu a je nazývána dvoufaktorovou autentizací. Proto bylo navrženo řešení s využitím čipových karet, které splňuje požadavky dané zákonem o kybernetické bezpečnosti č.181/2014 Sb. a jeho prováděcí vyhlášky č. 316/2014 Sb., konkrétně §18 - Nástroj pro ověřování identity uživatelů.
Karty obsahují kontaktní kryptografický čip, svůj vlastní operační systém a bezpečnou paměť na privátní klíče. Znamená to, že mohou veškeré kryptografické operace provádět mimo operační systém počítače, ke kterému jsou připojeny. Přístup ke službám operačního systému karty je umožněn pouze při zadáni PIN.
Bezkontaktní čip karet bude dále využity též jako vstupní karta v systému EKV pro identifikaci administrátorů a oprávněných osob přistupujících do prostor režimových pracovišť ICT.
Součástí tohoto řešení je jednak doplnění HW počítačů o čtečku čipové karty, je-li to nutné a za druhé implementace SW nutného pro práci s čipovou kartou. Nedílnou součástí je i zajištění procesů pro práci s kartami (vydávání karet, distribuce certifikátů, zaškolení uživatelů, zneplatnění karet, …). Toto opatření tak naváže na prostředky pořízené z jiného projektu, rozšíří jeho funkcionality a umožní karetní systém využívat pro více účelů.

Obrázek 16 - Čtečka čipových karet

Jako nejoptimálnější se jeví použití karet IDPrime 841, jejichž parametry naplňují požadavky zákona a splňují vysoké bezpečnostní standardy.

Čipová karta

Kontaktní část

- CC EAL5+
- QSCD
- Paměť pro certifikáty 50 KB
- Podpora Windows, MAC, Linux, Android, iOS
- Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits)
- Hash: SHA-1, SHA-256, SHA-384, SHA-512.
- RSA: up to RSA 2048 bits (and optionally up to 4096 bits)
- RSA OAEP & RSA PSS
- Elliptic curves: P-256, P-384, P-521 bits, ECDSA, ECDH
- On-card asymmetric key pair generation (RSA up to RSA2048 & Elliptic curves)
- Komunikační protokoly T=0, T=1, PPS, rychlost až 230 Kbps
- Životnost minimálně 500 000 cyklů zápisu/mazání

Bezkontaktní část

- DESFire EV1 4KB

Čtečka se snímačem čipové karty

Pro implementaci byla zvolena USB čtečka, která je s vybraným typem karet plně kompatibilní a její zprovoznění je primitivní a z administrátorského hlediska nenáročné.

- USB 2.0
- Podporované OS – Windows 10/8.1/8/7/Vista/Server 2012/Server 2008R2, Windows CE (5/6/7), Linux Debian 6.0+ / Ubuntu 11.04+/ Fedora 15+; Open SUSE 11.4+, Mac OS X; AndroidTM
- Podpora ISO 7816 Class A, B and C cards (5 V, 3 V, 1.8 V)
- 100,000 cyklů vložení
- EMV Level 1 mechanically compliant
- Podpora embosovaných karet

Obslužný SW

Na koncové zařízení – počítače, notebooky i administrátorské stanice bude instalován SW pro zajištění správného využití čipové karty. Nainstalován tak bude SafeNet Authentication Client a SafeNet Authentication Manager

- Podpora dvou faktorové autentizace
- Podpora Common Criteria a FIPS certifikovaných zařízení
- Podpora PIN Pad čteček
- Podpora pro plnou úpravu klienta, včetně bezpečnostní konfigurace, politik a uživatelského rozhraní
- Podpora virtuálních klávesnic
- Stejné rozhraní a používání na všech platformách
- Podpora Windows, MaxOS, Linux,
- Podpora PKCS#11 V2.20, MS CryptoAPI and CNG (CSP, KSP), Mac Keychain (TokenD), PC/SC
- Podpora 3DES, SHA-1, SHA-256, RSA up to 2048-bit, Elliptic Curve Cryptography (ECC)
- Podpora prohlížečů Firefox, Internet Explorer, Chrome
- Centrální management

8.1.17. 0patření č. 16 – Rozšíření stávajícího dohledového centra [redacted]

Pro zkvalitnění služeb stávajícího systému pro dohled nad infrastrukturou úřadu [redacted] je zapotřebí provést zkapacitnění technických prostředků, na kterých systém běží. Systém monitoringu slouží k detekci stavu infrastruktury a naplnění požadavků na vysokou dostupnost v rámci §26 - Nástroj pro zajišťování úrovně dostupnosti.

Umožňuje monitorovat operační systémy Windows, Linux, Unix a Mac OS. Řešení podporuje monitoring SNMP, WMI, plovoucí monitoring, stejně jako packet sniffing a zároveň veškerá zařízení s normami IPv4 a IPv6. Nabízí

přes 200 speciálně přednastavených sensorů vytvořených například pro QoS monitoring, dohled nad emaily, webovými prezentacemi, monitoring aplikací, databází, virtuálních prostředí a mnoho dalších....
[redacted] monitoruje všechny systémy, zařízení, provoz a aplikace IT infrastruktury pomocí těchto technologií:

- Ping
- SNMP: připravené k použití s možností vlastní
- WMI and Windows Performance Counters
- SSH: pro systémy Linux / Unix a MacOS
- Hlídání toků a Packet Sniffing
- HTTP požadavky a přijímaná data
- SQL

Síťový monitor[redacted] je primární sestávat ze dvou částí systému:

- Core Server – Jedná se o ústřední část instalace [redacted] a obsahuje data (Úložiště, webový server, nástroj pro vytváření zpráv, oznamovací systém a další)
- Sonda (y) - Část[redacted] na které se provádí skutečné sledování.

Všechna data monitorování jsou předávána centrálnímu jádrovému serveru.

[redacted]

8.1.18. 0patření č. 17 – Implementace testovacího centra

Pro zajištění dostupnosti všech služeb poskytovaných uživatelskými stanicemi i servery je bezpodmínečně nutné zamezit nežádoucím interakcím mezi nově nainstalovanými aplikacemi. Zejména je vhodné provádět tuto kontrolu u aplikací VIS a KII v rámci bezpečnostního testování dle §24, odst. 1, aby bylo zamezeno jakýmkoli nežádoucím interakcím s nimi ze strany jiných aplikací. V zájmu omezení vzniku potenciálních problémů v této

oblasti je vhodné doporučit provedení implementace nástroje, který bude schopen poskytnout komplexní soubor informací o akcích prováděných aplikacemi při instalacích, případně v rámci následné funkce v rámci operačního systému Windows. Uvedené řešení by mělo umožnit detekci změn provedených zkoumanými aplikacemi na úrovni souborového systému a registrů v rámci testovací sítě s odděleným přístupem od sítě provozní

8.1.19. 0patření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management

Pro zajištění schopnosti detekovat zranitelnosti podpůrných technických aktiv a rovněž pro zajištění schopnosti provádět bezpečnostní testy aplikací v kontextu §24, odst. 1, lze doporučit implementaci nástroje pro vulnerability management. Nástroj Rapid7 Nexpose Express nabízí možnost odhalovat zranitelnosti ve webových aplikacích, v operačních systémech a na úrovni služeb běžících na otevřených portech zkoumaného systému. Jako žádoucí se rovněž jeví schopnosti distribuovaného skenování a agent-based skenů.

8.2. V případě, že některá technická opatření budou sdílena systémy, žadatel podrobně a přehledně tuto situaci popíše v souladu s nastavenou cílovou hodnotou indikátoru.

Vzhledem k tomu, že projekt řeší bezpečnost infrastruktury Pardubického kraje jako celek, jsou bezpečnostní řešení navrhována komplexně a jednotlivá tachnická opatření jsou sdílena mezi více systémy. Dopady opatření na jednotlivé systémy jsou přehledně vidět z tabulky č. Tabulka 38 - Přehled systémů a opatření.

8.3. V případě, že některé technické opatření nahrazuje existující technické opatření, které není v souladu s vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnost, žadatel podrobně popíše, proč stávající technické řešení není v souladu s touto vyhláškou (relevantní pouze u KII/VIS/ISZS)

Žadatel nenahrazuje žádné stávající technické opatření, ale pouze ho doplňuje z důvodů redundace nebo jako nové řešení.

8.4. Byznys procesy pro výzvu 10

8.5. Popis procesů a ArchiMate Vizualizace

Zpracování Archimate vizualizací vybraných procesů naleznete v samostatné příloze „**A" - Archimate vizualizace**.

8.5.1. Business procesy pro opatření– Provedení GAP analýzy

a. Auditor provede interviu se spravci a majiteli aktiv
b. Auditor zpracuje rozdílovou analýzu
c. GAP analýza bude vstupem pro úpravu analýzy rizik - plán zvládání rizik - nápravná opatře

8.5.2. Business procesy pro opatření č. 1 - Implementace správy privilegovaných uživatelů a účtů

8.5.2.1. Povolení přístupu do PIM a přidělení oprávnění

a. Uživatel požádá prostřednictvím SD o zřízení přístupu do PIM
b. Ticket je směrován na nadřízeného zaměstnance ke schválení.
c. Nadřízený definuje skipiny oprávnění, ke kterým bude mít uživatel přístup.
d. Schválený ticket je předán administrátorovi PIM.

e. Administrátor povolí přístup pro uživatele do PIM a nastaví oprávnění pro všechny požadované skupiny.
f. Administrátor změny zaznamená do SD ticketu.

8.5.2.2. Odebrání PIM přístupu

a. Uživatel opouští organizaci a HR v procesu výpovědi vytvoří SD ticket na odstranění účtu v Active Directory. S jeho smazáním nebo zablokováním se automaticky zruší i PIM přístup.
b. Pomine-li nutnost mít PIM přístup nebo dojde k nutnosti změnit nastavená oprávnění, tak buď uživatel, nebo jeho nadřízený vytvoří v SD žádost o zrušení/změně PIM přístupu
c. Ticket je předán administrátorovi PIM
d. Administrátor zakáže/změní přístup v PIM nebo jeho oprávnění pro uživatele.
e. Administrátor změny zaznamená do SD ticketu.

8.5.3. Business procesy pro opatření č. 2 - Implementace VPN brány

8.5.3.1. Povolení VPN přístupu

a. Zaměstnanec požádá prostřednictvím SD o aktivaci dočasného VPN přístupu (zřízení VPN není předmětem tohoto procesu)
b. Ticket je předán administrátorovi Active Directory
c. Administrátor povolí VPN přístup pro uživatele a zajistí instalaci a konfiguraci VPN klientaAdministrátor změny zaznamená do SD ticketu.

8.5.3.2. Odebrání VPN přístupu

a. Uživatel opouští organizaci a HR v procesu výpovědi vytvoří SD ticket na odstranění účtu v Active Directory. S jeho smazáním nebo zablokováním se automaticky zruší i VPN přístup.
b. Pomine-li nutnost mít VPN přístup, tak buď uživatel, nebo jeho nadřízený vytvoří v SD žádost o zrušení VPN přístupu
c. Ticket je předán administrátorovi Active Directory
d. Administrátor povolí VPN přístup pro uživatele a nastaví automatickou odinstalaci VPN klienta ze zařízení uživatele.
e. Administrátor změny zaznamená do SD ticketu.

8.5.4. Business procesy pro opatření č. 3 - Zajištění redundance optických tras pro přístupové switche

a. Pracovník instalárora provede místní šetření a připraví návrh vedení kabelových tras
b. Odpovědný zástupce úřadu schválí návrh kabelových tras
c. Instalační firma provede úkony stavební připravenosti
d. Instalační firma instaluje kabelové žlaby a mikrotrubičky
e. Instalační firma zafoukne optická vlákna
f. Instalační firma provede instalaci a osazení kabelových van včetně navaření pigtail
g. Instalační firma provede měření optických tras
h. Instalační firma provede požární ucpávky v místech přechodů mezi požárními úseky
i. Instalační firma provede dokumentaci skutečného provedení
j. Instalační firma předá optické trasy odpovědnému pracovníkovi úřadu
k. Odpovědný pracovník úřadu provede kontrolu a potvrdí převzetí zhotoviteli

8.5.5. Business procesy pro opatření č. 4 - Doplnění přístupových přepínačů

8.5.5.1. Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě

a. 802.1x část
    i. přidělení/změna autorizačních oprávnění uživateli

ii. schválení nefiremního zařízení
iii. povolení zařízení kontraktora
iv. registrace/smazání pasivního zařízení
v. vyhodnocení kybernetické události/incidentu

b. administrace zařízení
vi. přidělení/změna oprávnění administrace
vii. odebrání oprávnění administrace
viii. audit přístupů na prvky a změn v konfigurace

8.5.5.2. Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě

a. 802.1x část
i. Přidělení/změna autorizačních oprávnění uživateli
ii. Zaměstnanec nastoupí do zaměstnání nebo mění pozici.
iii. HR oddělení zařazuje zaměstnance do skupiny v IDM podle jeho organizačního zařazení.
iv. IDM propisuje tyto informace do AD.
v. Autentizační systém aplikuje autorizační pravidla v síti podle informací v AD.

b. Schválení nefiremního zařízení/ povolení zařízení kontraktora
i. Zaměstnanec vytvoří žádost o schválení nefiremního zařízení do SD.
ii. SD ticket je předán na nadřízeného zaměstnance.
iii. Pokud je požadavek schválen, je předán administrátorovi AAA zařízení.
iv. V autentizačním systému je vytvořen záznam, opravňující přístup zařízení do sítě.
v. Administrátor změny zaznamená do SD ticketu.

c. Registrace/smazání pasivního zařízení
i. Administrátor, který spravuje danou třídu zařízení, se připojí k AAA systému a zaregistruje nebo smaže záznam, který opravňuje přístup pasivního zařízení do sítě.

8.5.6. Business procesy pro opatření č. 5 - Doplnění HW Datového centra o servery a pole

8.5.6.1. Vytvoření virtuálního serveru

a. Vlastník aktiva požádá prostřednictvím SD o vytvoření virtuálního serveru.
- obsahem tiketu je zdůvodnění požadavku na vytvoření virtuálního serveru
- v tiketu jsou uvedené technické požadavky na parametry virtuálního serveru

b. Tiket je směrován na vedoucího odboru, pod který spadá vlastník aktiva. Ten ho po schválení předá na architekta.

c. Architekt posoudí požadavek z hlediska bezpečnosti a požadovaných funkčních parametrů
i. V případě, že je vše v souladu z bezpečnostní politikou, tak je požadavek předán na správce datového centra
ii. V případě, že je požadavek v nesouladu s bezpečnostní politikou, nebo je vyžadována jejich zásadní změna, tak je požadavek předán k posouzení manažerovi kybernetické bezpečnosti.

d. Správce datového centra požadavek posoudí a pokud požadovaná služba není v nesouladu s pravidly provozu, tak je předá na administrátory, kteří zajistí vlastní konfiguraci:
- administrátory virtualizační platformy
- administrátory operačního systému
- administrátory aplikací
- administrátory bezpečnostních prvků
- administrátory síťových prvků

e. Po předání na jednotlivé administrátory všech dotčených komponent, tak je provedeno jejich nastavení
i. administrátor virtualizační platformy vytvoří virtuální server

ii. administrátor operačních systémů provede instalaci OS na daný virtuální stroj
iii. správce aplikace provede její konfiguraci
iv. administrátor bezpečnostních prvků provede jejich nastavení pro povolení požadované komunikace
v. správce síťových prvků provede jejich upravu konfigurace, pro zajištění datové konektivity u nového serveru

f. Veškeré úpravy provedené jednotlivými administrátory zaznamenají do tiketu a upraví dokumentaci svých spravovaných komponent
g. Virtuální server je předán vlastníkovi aktiva k užívání

8.5.6.2. Smazání virtuálního serveru

a. Vlastník aktiva požádá prostřednictvím SD o smazání virtuálního serveru.
   - obsahem tiketu je zdůvodnění požadavku proč má být virtuální server smazán
b. Tiket je směrován na vedoucího odboru, pod který spadá vlastník aktiva. Ten ho musí schválit.
c. Schválený tiket je předán na architekta, který posoudí relevantnost požadavku.
d. Architekt posoudí požadavek z hlediska bezpečnosti a požadovaných funkčních parametrů

   i. V případě, že je vše v souladu z bezpečnostní politikou, tak je požadavek předán na administrátory, kteří zajišťují vlastní konfiguraci.
      - virtualizační platformy
      - operačního systému
      - aplikací
      - bezpečnostních prvků
      - síťových prvků

   ii. V případě, že je požadavek v nesouladu s bezpečnostní politikou, nebo je vyžadována jejich zásadní změna, tak je požadavek předán k posouzení manažerovi kybernetické bezpečnosti.

e. Po předání na jednotlivé administrátory všech dotčených komponent, tak je provedeno jejich nastavení

   i. správce aplikace provede zálohování konfigurací aplikace v případě potřeby, případně odstraní vazby na odstraňovanou aplikaci z jiných systémů
   ii. administrátor bezpečnostních prvků odstraní již nepotřebná pravidla
   iii. správce síťových prvků provede odstranění nepotřebné konfigurace
   iv. administrátor virtualizační platformy odstraní virtuální server

f. Veškeré úpravy provedené jednotlivými administrátory zaznamenají do tiketu a upraví dokumentaci svých spravovaných komponent

8.5.7. Business procesy pro opatření č. 6 - Řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě

8.5.7.1. Implementace aplikace MABKEEPER

8.5.7.1.1. Nefunkční přístup interního uživatele

a. Uživatel zadává požadavek na podporu (osobně, telefonicky), že se nemůže přihlásit do sítě z důvodu chybné autentizace
b. Správce ho ověří (osobně, nebo na základě, znalosti username uživatele, MAC adresy jeho PC a osobního čísla)
c. Správce zakládá tiket v SD
d. Správce povolí dočasně komunikaci koncovému zařízení, které se nedaří ověřit pomocí 802.1x pomocí vyjímky na MAC adresu zařízení
e. Správce provede diagnostiku a odstranění chyby
f. Po odstranění problémů je vyjímka MAC adresu odstraněna

8.5.7.1.2. Zajištění přístupu pro externího uživatele/kontraktora

a. Sponzor zadává požadavek do SD, který je směřován na svého nadřízeného
b. Schválený ticket je směřéván na správce aplikace MABKEEPER
c. Správce povolí dočasně komunikaci koncovému zařízení pomocí vyjímky na MAC adresu zařízení externisty/kontraktora. Vyjímka je povolena pouze na striktně definovanou dobu
d. Správce zaznamená změny do SD

8.5.7.2. Implementace aplikace OFFICELOCATOR

a. S aplikací pracuje pouze její správce
b. Správce provádí při potřebě:
    i. Sledování stavu koncového zařízení
    ii. Vynucení reautentizace koncového zařízení
    iii. Audit chování koncových stanic

8.5.8. Business procesy pro opatření č. 7 – Centrální logovací nástroj

8.6.1.1 Povolení přístupu do Log managementu a přidělení oprávnění

g. Uživatel požádá prostřednictvím SD o zřízení přístupu do Log managementu
h. Ticket je směrován na nadřízeného zaměstnance ke schválení.
i. Nadřízený definuje skupiny oprávnění, ke kterým bude mít uživatel přístup.
j. Schválený ticket je předán administrátorovi Log managementu.
k. Administrátor povolí přístup pro uživatele do Log managementu a nastaví oprávnění pro všechny požadované skupiny.
l. Administrátor změny zaznamená do SD ticketu.

a. Uživatel zadává požadavek na podporu (osobně, telefonicky), že se nemůže přihlásit do sítě z důvodu chybné autentizace
b. Správce ho ověří (osobně, nebo na základě, znalosti username uživatele, MAC adresy jeho PC a osobního čísla)
c. Správce zakládá tiket v SD
d. Správce povolí dočasně komunikaci koncovému zařízení, které se nedaří ověřit pomocí 802.1x pomocí vyjímky na MAC adresu zařízení
e. Správce provede diagnostiku a odstranění chyby
f. Po odstranění problémů je vyjímka MAC adresu odstraněna
g. Vyřešení problému je zaznamenáno do SD

8.6.1.2 Odebrání přístupu do Log managementu

f. Uživatel opouští organizaci a HR v procesu výpovědi vytvoří SD ticket na odstranění účtu v Active Directory. S jeho smazáním nebo zablokováním se automaticky zruší i Log management přístup.
g. Pomine-li nutnost mít přístup do Log managementu nebo dojde k nutnosti změnit nastavená oprávnění, tak buď uživatel, nebo jeho nadřízený vytvoří v SD žádost o zrušení/změně přístupu
h. Ticket je předán administrátorovi Log managementu.
i. Administrátor zakáže/změní přístup v Log managementu nebo jeho oprávnění pro uživatele.
j. Administrátor změny zaznamená do SD ticketu.

8.5.9. Business procesy pro opatření č. 8 - Implementace vysoké dostupnosti [redacted]

8.5.9.1. Replikace dat

a. Proběhne detekce změněných v definovaném časovém okně
b. Replikace změněných dat do záložní databáze
c. Zpětné ověření, že se data korektně replikovala

8.5.10. Business procesy pro opatření č. 9 - Implementace řešení pro monitorování toků

8.5.10.1. Řešení pro monitorování toků - Upozornění na bezpečnostní incident

a. V případě incidentu behaviorální aplikace pošle email na zadanou adresu (emailová adresa Analytika)
b. Analytik se přihlásí do bezpečnostního portálu na kolektoru
c. Analytik zkontroluje zda se nejedná o "false positive" událost
d. V případě "false positive" události Analytik upraví konfiguraci behaviorální aplikace na kolektoru
e. V případě, že se nejedná o "false posisitve" událost, tak zadá tiket do SD.
f. V SD si tento tiket převezme řešitel pro danou oblast.

8.5.10.2. Řešení pro monitorování toků - Pravidelná kontrola portálu kolektoru

a. Analytik dvakrát denně kontroluje portál kolektoru, zda se nevyskytují nějaké anomálie v monitoringu toků
b. Současně s kontrolou portálu kolektoru zkontroluje i bezpečnostní portál
c. Pokud analytik zjistí nějaké nesrovnalosti, tak vytvoří tiket v SD.
d. V SD si tiket převezme řešitel pro danou oblast.

8.5.10.3. Řešení pro monitorování toků - Zjištění informací o komunikaci do Internetu

a. V případě potřeby zjistit informace o komunikaci do internetu, zadá Analytik čas a a cílovou adresu do vyhledávacího pole
b. Aplikace vygeneruje report s informacemi o adrese uživatele, která odpovídá zadanému filtru

8.5.11. Business procesy pro opatření č. 10 - Doplnění redundantní [redacted] proxy

8.5.11.1. Vytvoření přístupu do Internetu

a. Zaměstnanec požádá prostřednictvím SD o aktivaci Internet přístupu
b. Ticket je směrován na nadřízeného zaměstnance ke schválení.
c. Schválený ticket je předán administrátorovi Active Directory
d. Administrátor povolí Internetový přístup pro uživatele tím, že ho zařadí do příslušné skupiny v MS Active Directory.
e. Administrátor změny zaznamená do SD ticketu.

8.5.11.2. Odebrání přístupu do Internetu

a. Uživatel opouští organizaci a HR v procesu výpovědi vytvoří SD ticket na odstranění účtu v Active Directory. S jeho smazáním nebo zablokováním se automaticky zruší i Internetový přístup.
b. Pokud pomine mít Internetový přístup, tak buď uživatel, nebo jeho nadřízený vytvoří v SD žádost o zrušení přístupu
c. Ticket je předán administrátorovi Active Directory
d. Administrátor zakáže Internetový přístup pro uživatele.
e. Administrátor změny zaznamená do SD ticketu.

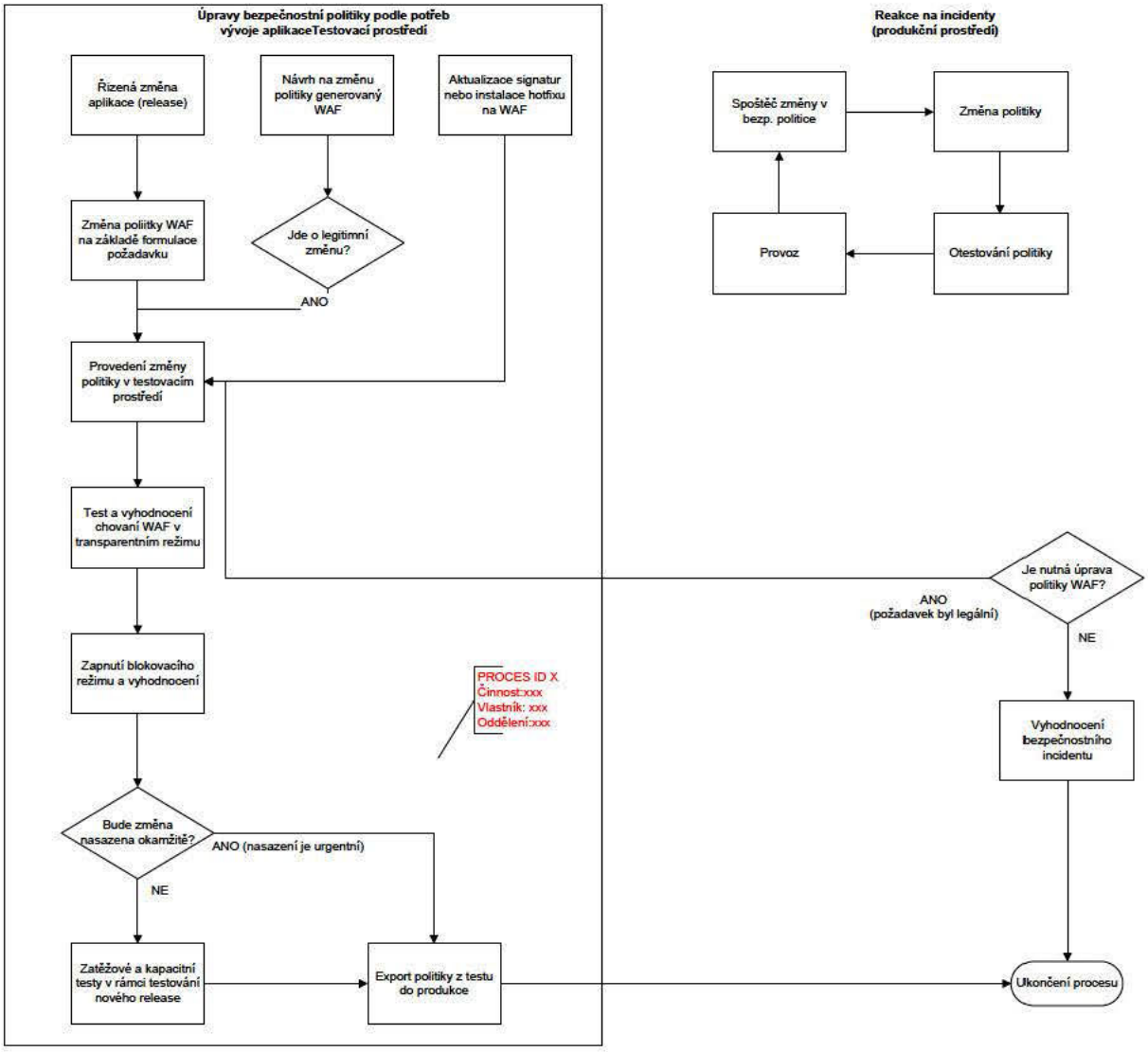
8.5.12. Business procesy pro opatření č. 11 - Rozšíření [redacted] o SANDBOX

8.5.12.1. Kontrola souborů pomocí sandbox technologie ve WWW provozu (HTT, HTTPS, FTP)

a. Aplikace požádá WWW server o stažení souborů
b. Tento požadavek předá proxy server na cílový server
c. Cílový server pošle požadovaný soubor na proxy server
d. Proxy server předá požadovaný soubor k analýze sandboxovacímu nástroji

e. Pokud je soubor nezávadný, tak se předá proxy serveru a ten pak aplikaci, která tento soubor požadovala.
f. Pokud je soubor závadný, tak se soubor zablokuje a předá se zpráva o zablokování proxy serveru. Ten zobrazí aplikaci, která soubor požadovala, chybovou zprávu.

8.5.13. Business procesy pro opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru



8.5.14. Business procesy pro opatření č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS

8.5.14.1. Logování aktivit uživatelů

a. Veškeré operace uživatelů budou zaznamenány a zaslány na centrální logger.

8.5.14.2. Logování aktivit administrátorů

a. Veškeré operace administrátorů budou zaznamenány a zaslány na centrální logger.

8.5.14.3. Proces doložení autenticity dokumentu:

a. Autorita (např. soud) požádá o elektronický dokument evidovaný ve spisové službě

b. Odborný referent uloží příslušný dokument na nosič dat
c. Správce SSL doloží dotčené transakční protokoly
d. Odborný referent předá všechny materiály autoritě

8.5.14.4. Proces evidence el. dokumentu na podatelně:

a. Referent podatelny kontroluje a příjme podaní z externího zdroje (DS, mail)
b. Systém uloží došlou zprávu vč. příloh do úložiště el. dokumentů
c. Referent podatelny doplní metadata o došlém dokumentu a předá ke zpracování

8.5.14.5. Proces evidence vlastního el. dokumentu:

a. Referent vyplní metadata o vlastním dokumentu
b. Referent uloží el. obraz dokumentu do úložiště
c. Další zpracování (předání, odeslání, uložení)

8.5.15. Business procesy pro opatření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů

8.5.15.1. Komunikace mezi aplikací GINIS a uložištěm zákazníka

a. V případě přenosu dokumentů mezi aplikací GINIS a datovým uložištěm zákazníka, dojde k zašifrování obsahu při jeho přenosu.

8.5.16. Business procesy pro opatření č. 15 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů

8.5.16.1. Vydání čipové karty

a. Zaměstnanci vznikne z výkonu funkce nárok na čipovou kartu
b. Pracovnice/k personálního oddělení zadá personální data do centrálního systému
c. Pracovnice/k personálního oddělení vytiskne čipovou kartu
d. Pracovnice/k personálního oddělení zadá prostřednictvím helpdesku požadavek na vystavení certifikátu a jeho nahrání do na kartu
e. Schválený ticket je předán administrátorovi Active Directory
f. Administrátor vygeneruje certifikát pro uživatele a nahraje jej na kartu
g. Administrátor provede nastavení uživatele v centrálním systému
h. Administrátor zaznamená změny do helpdesk systému a uzavře ticket.
i. Administrátor předá kartu zpět na personální oddělení
j. Pracovnice/k personálního oddělení předá kartu uživateli
k. Pracovník zadá ke kartě PIN a formálně převezme kartu

8.5.16.2. Přihlášení do systému

a. Uživatel vloží kartu do čtečky čipových karet
b. Obslužný SW zobrazí požadavek na zadání PIN
c. Uživatel zadá PIN k čipové kartě
d. Operační systém karty předá obslužnému SW certifikát, kterým je provedena autentizace

8.5.16.3. Zneplatnění karty

a. Pracovnice/k personálního oddělení zadá prostřednictvím helpdesku požadavek na zneplatnění karty
b. Pracovnice/k personálního oddělení provede nastavení uživatele v systému EKV
c. Administrátor provede nastavení uživatele v centrálním systému a zneplatní certifikát na certifikační autoritě
d. Administrátor zaznamená změny do helpdesk systému a uzavře ticket
e. Uživatel vrátí kartu úřadu

8.5.17. Business procesy pro opatření č.16 - Rozšíření stávajícího dohledového centra [redacted]

8.5.17.1. Pravidelná kontrola monitoringu systému

a. Pracovnice/k monitoringu provádí průběžnou proaktivní kontrola na infrastruktury sledováním
b. Pracovnice/k monitoringu zajišťuje sledování metrik a SLA

8.5.17.2. Konfigurace

a. Administrátor naváže systém na současnou infrastruktury
b. Konfigurace senzorů
c. Nastavení dohledu a reportingu (email / SMS) vydefinování trash holdů
d. Definice monitoring operátorů
e. Administrátor Infrastruktury a bezpečnostní administrátor definuje rozsahu monitoringu
f. Administrátor systému [redacted] provede nastavení metrik dohledu a nasatvení metriky SLA
g. Požadavek na přidání nového HW do monitoringu
h. Zařazení nových prvků do [redacted]

8.5.17.3. Údržba [redacted] systému

a. Kontrola funkčnosti systému (běh aplikace centrálního systému a sond, úložný prostor na HDD, výkon procesorů, zaplnění paměti)
b. Implemenatce systémových patchí
c. Instalace nových update

8.5.18. Business procesy pro opatření č. 17 - Implementace testovacího centra

8.5.18.1. Realizace testu s využitím nástrojů

a. Zachycení stavu systému (provedení snapshotu)
b. Start testované aplikace (instalace, provedení změn, atd.)
c. Zachycení stavu systému (provedení snapshotu)
d. Porovnání obou zachycených stavů
e. Analýza výsledných rozdílů zachycených stavů

8.5.19. Business procesy pro opatření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management

8.5.19.1. Ad-hoc vulnerability scan

a. Stanovení cílů pro scanovení
b. Stanovení rozsahu a typu scanu (zranitelnosti, otevřené porty, atp.)
c. Provedení scanu
d. Interpretace výsledků scanu (vyhodnocení)
e. Realizace nápravných opatření
f. Opakování scanu pro ověření funkce realizovaných opatření

8.5.19.2. Periodický vulnerability scan

a. Stanovení cílů a periody pro scanovení
b. Stanovení rozsahu a typu scanu (zranitelnosti, otevřené porty, atp.)
c. Provedení scanu
d. Průběžná interpretace výsledků scanu (vyhodnocení)
e. Realizace nápravných opatření

9. Výčet systémů zabezpečovaných v rámci projektu

9.1. Přehledný a stručný seznam KII/VIS/ISZS/IS/KS, které žadatel zabezpečí v rámci projektu

V rámci projektu budou zabezpečovány všechny níže uvedené systémy včetně významného informačního systému daného přílohou č. 1 vyhlášky 317/2014 sb., :

PČ	*Název VIS*	*Popis*
107	**Integrovaný informační systém GINIS**	Modulárnísystém GINIS společnosti Gordic. Pokrývá oblasti rozpočtu, účetnictví, majetku, dotace, styk s bankami, smlouvy, spisová služba a další moduly související s provozem úřadu

Tabulka 17 - Zabezpečený Významný informační systém Pardubického kraje

GINIS je souhrný název pro cca 50 samostatných aplikačních modulů spojených do jedné programové platformy. V jednotlivých modulech integrovaného informačního systému pracuje každodenně přes 95% uživatelů sítě Pardubického kraje a tento systém zasahuje do všech technických aktiv infrastruktury Pardubického kraje.

9.2. Systémy, které nejsou jednoznačně vymezeny legislativou, tj. IS a KS, musí žadatel jednoznačně definovat a učit v této kapitole nebo s odkazem na kapitolu 5. IS musí naplňovat znaky informačního systému, KS musí naplňovat znaky komunikačního systému.

Tyto systémy jsou uvedeny v Tabulce 18:

Název systému	*Typ*
Informační systém Krajského úřadu Pardubického kraje	IS
Emailový systém	KS
Webový portál Pardubického kraje	IS
Formulářový systém sběru dat z obcí	IS
Sběrové ekonomické výkazové automaty	KS
Hostovaná spisová služba	IS
Krajské digitální úložiště	IS
GIS mapové servery	IS
ISZR kukátko	IS

Tabulka 18 – Přehled zabezpečených systémů IS/KS

VIS je definován dle vyhlášky č.317/2014 Sb., IS a KS jsou jednoznačně definovány v kapitole 5

10. Plnění technických opatření

Předkládaným projektem bude realizováno několik bezpečnostních technických opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Konkrétně jde o opatření:

- §17 - Nástroj pro ochranu integrity komunikačních sítí
- §18 - Nástroj pro ověřování identity uživatelů
- §19 - Nástroj pro řízení přístupových oprávnění
- §20 - Nástroj pro ochranu před škodlivým kódem
- §21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- §22 - Nástroj pro detekci kybernetických bezpečnostních událostí
- §23 - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- §24 - Aplikační bezpečnost
- §25 - Kryptografické prostředky
- §26 - Nástroj pro zajišťování úrovně dostupnosti

Tato studie definuje následující technická opatření, která jsou dále popisována v rámci tohoto dokumentu. Požadavky Průběžné výzvy č. 10 IROP vyžadují, že každý projekt musí realizovat minimálně jedno bezpečnostní technické opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Projekt Bezpečnost komunikační infrastruktury identifikuje celkem 10 technických opatření, která jsou v rámci studie popsána 18 řešeními viz tabulky níže.

ID opatření:	1
Oblast opatření podle ZKB:	§18 - Nástroj pro ověřování identity uživatelů §21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko

Název opatření:	Implementace správy privilegovaných uživatelů a účtů
Stručný popis opatření:	Implementace systému pro management privilegovaných účtů a management přístupu třetích stran. Umožňuje řídit a monitorovat činnosti a oprávnění administrátorů I externích dodavatelů s vysokými právy. Detaily viz kapitola 8.1.3
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 19 - Technické opatření č. 1

ID opatření:	2
Oblast opatření podle ZKB:	§17 - Nástroj pro ochranu integrity komunikačních sítí §18 - Nástroj pro ověřování identity uživatelů §25 - Kryptografické prostředky
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Implementace VPN brány
Stručný popis opatření:	Toto opatření bude realizováno implementací VPN brány, která zajistí šifrovaný vzdálený přístup pro interní zaměstnance i externí dodavatele k aplikacím spadajícím do VIS. Zároveň bude sloužit i pro vzdálenou správu podpůrných aktiv.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 20 - Technické opatření č. 2

ID opatření:	3
Oblast opatření podle ZKB:	§26 - Nástroj pro zajišťování úrovně dostupnosti
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Zajištění redundance optických tras pro přístupové switche
Stručný popis opatření:	Bude provedeno Doplnění optické kabeláže pro zajištění druhé, redundantní trasy mezi přístupovými a centrálními prvky. Detaily viz kapitola 8.1.5

Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 21 - Technické opatření č. 3

ID opatření:	4
Oblast opatření podle ZKB:	§17 - Nástroj pro ochranu integrity komunikačních sítí §18 - Nástroj pro ověřování identity uživatelů §19 - Nástroj pro řízení přístupových oprávnění §22 - Nástroj pro detekci kybernetických bezpečnostních událostí §25 - Kryptografické prostředky §26 - Nástroj pro zajišťování úrovně dostupnosti
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Doplnění přístupových přepínačů
Stručný popis opatření:	Toto opatření bude realizováno náhradou nepodporovaných přepínačů výrobcem, zbudováním záložních datových tras mezi páteřní a přístupovou částí sítě, odesíláním informací o datovém provozu do centrálního kolektoru k vyhodnocení. A šifrováním provozu na druhé vrstvě mezi centrální lokalitou a vzdálenou lokalitou spisovny.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 22 - Technické opatření č. 4

ID opatření:	5
Oblast opatření podle ZKB:	§26 - Nástroj pro zajišťování úrovně dostupnosti
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko

Název opatření:	Doplnění HW Datového centra o servery a pole
Stručný popis opatření:	Toto opatření bude realizováno implementací řešením prostředků datových center v obou lokalitách. Konkrétně se bude jednat o dvojici páteřních přepínačů v každé lokalitě, serverů s operačními systémy v podobě [redacted] nebo Microsoft Windows server a diskového systému v podobě stretched metro clusteru. Opatření bude použito pro běh aplikací a ukládání dat vyplývajících z jiných opatření.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 23 - Technické opatření č. 5

ID opatření:	6
Oblast opatření podle ZKB:	§18 - Nástroj pro ověřování identity uživatelů §19 - Nástroj pro řízení přístupových oprávnění
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě
Stručný popis opatření:	Toto opatření bude realizováno implementací systému, který zajistí Autentizaci a Autorizaci uživatelů, kteří budou mít možnost pracovat s centrální databází MAC adres zařízení. Díky aplikaci každá MAC adresa, která není označena jako pasivní zařízení, bude mít nastaven příznak expirace. Po jejím vypršení dojde k jejímu smazání.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 24 - Technické opatření č. 6

ID opatření:	7
Oblast opatření podle ZKB:	§18 - Nástroj pro ověřování identity uživatelů §19 - Nástroj pro řízení přístupových oprávnění
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba

	Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Centrální logovací nástroj
Stručný popis opatření:	Toto opatření bude realizováno implementací nástroje pro zajištění centrálního sběru logů ze všech systému i podpůrné infrastruktury.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI.

Tabulka 25 - Technické opatření č. 7

ID opatření:	8
Oblast opatření podle ZKB:	§26 - Nástroj pro zajišťování úrovně dostupnosti
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS
Název opatření:	Implementace vysoké dostupnosti pro [redacted]
Stručný popis opatření:	Toto opatření bude realizováno implementací replikace [redacted] databáze na záložní HW pomocí sady replikačních skriptů
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 26 - Technické opatření č. 8

ID opatření:	9
Oblast opatření podle ZKB:	§20 - Nástroj pro ochranu před škodlivým kódem §22 - Nástroj pro detekci kybernetických bezpečnostních událostí
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Implementace řešení pro monitorování toků
Stručný popis opatření:	Toto opatření bude realizováno implementací netflow kolektoru, který umožňuje interpretaci a grafické znázornění nasbíraných informací o datových tocích. Dále toto zařízení umožňuje upozornit na bezpečnostní rizika v síti pomocí nastavených akcí - např. zasláním emailu.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 27 - Technické opatření č. 9

ID opatření:	10
Oblast opatření podle ZKB:	§17 - Nástroj pro ochranu integrity komunikačních sítí §20 - Nástroj pro ochranu před škodlivým kódem §26 - Nástroj pro zajišťování úrovně dostupnosti
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Implementace doplnění redundantní [redacted] proxy
Stručný popis opatření:	Toto opatření bude realizováno implementací nové web proxy brány, která zajistí ochranu uživatelského webového provozu před škodlivým kódem. Dále bude tato nová [redacted] proxy sloužit pro zajištění vysoké dostupnosti stávajícího proxy řečení. Proxy řešení primárně chrání provoz z uživatelských stanic, které pracují s VIS systémy.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 28 - Technické opatření č. 10

ID opatření:	11
Oblast opatření podle ZKB:	§20 - Nástroj pro ochranu před škodlivým kódem
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Rozšíření [redacted] o SANDBOX
Stručný popis opatření:	Toto opatření bude realizováno implementací sendboxovacích brány, která zajistí ochranu uživatelského webového provozu před škodlivým kódem. Sendboxovací zařízení budou dostávat podezřelé soubory k analýze ze stávajících proxy serverů. Sendboxing bude sloužit ochranně provozu z uživatelských stanic, které pracují s VIS systémy a provozu z podpůrných aktiv VIS, které musí komunikovat do Internetu.

Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 29 - Technické opatření č. 11

ID opatření:	12
Oblast opatření podle ZKB:	§22 - Nástroj pro detekci kybernetických bezpečnostních událostí §24 - Aplikační bezpečnost §26 - Nástroj pro zajišťování úrovně dostupnosti
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Implementace Webového aplikačního firewallu a Loadbalanceru
Stručný popis opatření:	Toto opatření bude realizováno implementací dvou kusů Webových aplikačních firewalů, které zajistí ochranu až do úrovně L7 a zároveň umožní loadbalancing provozu DC.
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 30 - Technické opatření č. 12

ID opatření:	13
Oblast opatření podle ZKB:	§21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS
Název opatření:	Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS
Stručný popis opatření:	Toto opatření bude realizováno implementací GINIS modulu, který zajistí potřebnou úroveň logování pro všechny moduly systému GINIS
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 31 - Technické opatření č. 13

ID opatření:	14
Oblast opatření podle ZKB:	§25 - Kryptografické prostředky
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS

Název opatření:	Doplnění konektoru [redacted] pro úložiště elektronických dokumentů
Stručný popis opatření:	Toto opatření bude realizováno implementací konektoru společnosti Gordic zajišťujícího bezpečný přenos dat mezi systémem GINIS a uložištěm [redacted].
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 32 - Technické opatření č. 14

ID opatření:	15
Oblast opatření podle ZKB:	§18 - Nástroj pro ověřování identity uživatelů
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém GIS mapové servery ISZR kukátko
Název opatření:	Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů
Stručný popis opatření:	Toto opatření bude realizováno implementací druhého faktoru autentizace ve formě čipových karet a na nich uloženého certifikátu
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 33 - Technické opatření č. 15

ID opatření:	16
Oblast opatření podle ZKB:	§26 - Nástroj pro zajišťování úrovně dostupnosti
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Rozšíření stávajícího dohledového centra [redacted]
Stručný popis opatření:	Migrace stávajícího řešení monitorovacího systému [redacted] užívaného úřadem na hardwarové prostředky nově doplňovaného DC řešení popisované v opatření č. 7 této studie. Detaily viz. kpitola 8.1.19
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 34 - Technické opatření č. 16

ID opatření:	17

Oblast opatření podle ZKB:	§24 - Aplikační bezpečnost
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Implementace testovacího centra
Stručný popis opatření:	Implementace nástroje poskytujícího komplexní soubor informací o akcích prováděných aplikacemi při instalacích a případně v rámci následné funkce v rámci operačního systému Windows. Detaily viz. kpitola 8.1.20
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 35 - Technické opatření č. 17

ID opatření:	18
Oblast opatření podle ZKB:	§24 - Aplikační bezpečnost
KII/VIS/ISZS/IS/KS:	Integrovaný informační systém GINIS Informační systém Krajského úřadu Pardubického kraje Emailový systém Webový portál Pardubického kraje Formulářový systém sběru dat z obcí Sběrové ekonomické výkazové automaty Hostovaná spisová služba Krajské digitální úložiště GIS mapové servery ISZR kukátko
Název opatření:	Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management
Stručný popis opatření:	Implementace nástroje schopného detekovat zranitelnosti podpůrných technických aktiv a provádět bezpečnostní testy aplikací
Sdílení opatření se ISOUI:	Opatření není sdíleno s žádným ISOUI

Tabulka 36 - Technické opatření č. 18

10.1. Systémy sdílející technická opatření

Název systému	*Popis*
Informační systém Krajského úřadu Pardubického kraje	informační systém spojený z několika aplikací běžné denní agendy úředníků a zaměstnanců. Systém doplňuje svými funkcemi VIS

	GINIS a stejně jako on spolupracuje i s informačními systémy státu (ISZR, JIP/KAAS)
Emailový systém	komunikační systém úřadu je veden jako jedno z primárních aktiv úřadu. I přes fungující systém datových schránek je to stále nejrozšířenější médium pro komunikaci občana a komerčních subjektů s úřadem nebo opačně
Webový portál Pardubického kraje	www.pardubickykraj.cz - portál je hlavním informačním médiem spojujícího úřad s občanem. Z hlediska důvěryhodnosti a dostupnosti informací je tak veden jako jedno z primárních aktiv.
Formulářový systém sběru dat z obcí	informační systém spolupracující se starosty všech obcí Pardubického kraje. Systém shromažďuje kontaktní informace, které po ověření jsou k dispozici jednotlivým agendám úřadu.
Sběrové ekonomické výkazové automaty	automatický komunikační systém spojující na jedné straně obce a organizace veřejné správy, na druhé straně Centrální systém účetních informací státu (CSÚIS). Systém data přijímá, kontroluje a po kompletaci zasílá na CSÚIS
Hostovaná spisová služba	informační systém spisové služby plně zveřejněný vně úřadu využívaný zřizovanými organizacemi Pardubického kraje. Systém spolupracuje s dalšími systémy, jako jsou například základní registry
Krajské digitální úložiště	informační systém umožňující identifikaci osoby, která využije úložiště pro datovou komunikaci z internetu. Systém slouží vedle webového portálu jako nástroj výměny dat velké velikosti nebo vyššího zabezpečení
GIS mapové servery	informační systém prezentující mapové podklady občanům a organizacím. Tvorba mapových podkladů včetně doplňujících metadat je jedna z činností oddělení informatiky Pardubického kraje.
ISZR kukátko	informační systém umožňující zabezpečený přístup do systému základních registrů a vyčítání informací nutných k přenesené i samostatné působnosti úřadu. Systém tak naplňuje povinnosti kladené na úřad platnou legislativou

Tabulka 37 - Systémy sdílející technická opatření

	Integrovaný informační systém GINIS	Informační systém Krajského úřadu Pardubického kraje	Emailový systém	Webový portál Pardubického kraje	Formulářový systém sběru dat z obcí	Sběrové ekonomické výkazové automaty	Hostovaná spisová služba	Krajské digitální úložiště	GIS mapové servery	ISZR kukátko

	VIS	IS	KS	IS	IS	KS	IS	IS	IS	IS
Opatření č. 1 - Implementace správy privilegovaných uživatelů a účtů	X	X	X	X	X	X	X	X	X	X
Opatření č. 2 - Implementace VPN brány	X	X	X	X	X	X	X	X	X	X
Opatření č. 3 - Zajištění redundance optických tras pro přístupové switche	X	X	X	X	X	X	X	X	X	X
Opatření č. 4 – Doplnění přístupových přepínačů	X	X	X	X	X	X	X	X	X	X
Opatření č. 5 - Doplnění HW Datového centra o servery a pole	X	X	X	X	X	X	X	X	X	X
Opatření č. 6 – Implemetace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě	X	X	X	X	X	X	X	X	X	X
Opatření č. 7 – Centrální logovací nástroj	X	X	X	X	X	X	X	X	X	X
Opatření č. 8 - Implementace vysoké dostupnosti pro [redacted]	X	-	-	-	-	-	-	-	-	-
Opatření č. 9 - Implementace řešení pro monitorování toků	X	X	X	X	X	X	X	X	X	X
Opatření č. 10 – Doplnění redundantní [redacted] proxy	X	X	X	X	X	X	X	X	X	X
Opatření č. 11 – Rozšíření [redacted] o SANDBOX	X	X	X	X	X	X	X	X	X	X
Opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru	X	X	X	X	X	X	X	X	X	X
Opatření č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS	X	-	-	-	-	-	-	-	-	-
Opatření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů	X	-	-	-	-	-	-	-	-	-
Opatření č. 15 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů	X	X	X	-	-	-	-	-	X	X
Opatření č. 16 – Rozšíření stávajícího dohledového centra [redacted]	X	X	X	X	X	X	X	X	X	X
Opatření č. 17 - Implementace testovacího centra	X	X	X	X	X	X	X	X	X	X
Opatření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování – Vulnerability management	X	X	X	X	X	X	X	X	X	X

Tabulka 38 - Přehled systémů a opatření

11. Dlouhodobý majetek, pojištění

11.1. Dlouhodobý investiční majetek vstupující do projektu

V průběhu realizační etapy bude pořízen hmotný i nehmotný investiční majetek. V tabulce jsou uvedeny stavy aktiv a pasiv na konci realizační etapy. Neinvestiční náklady Projektu, které nebudou vstupovat do pořizovací ceny majetku, nejsou v tabulce uvedeny (osobní náklady, náklady na služby).

Aktiva	Prosinec 2017	Prosinec 2018	Říjen 2019	Pasiva	Prosinec 2017	Prosinec 2018	Říjen 2019
stálá aktiva	0	0	50 307	cizí zdroje	0	0	45 276
- techn. zhod.	0	0	0				
- hardware	0	0	44 869	dotace IROP	0	0	42 761
- software	0	0	5 438	státní rozpočet	0	0	2 515
oběžná aktiva	0	0	0	vlastní zdroje kraje	0	0	5 031
aktiva celkem	**0**	**0**	**50 307**	**pasiva celkem**	**0**	**0**	**50 307**

Tabulka 39 Plánované sestavy aktiv a pasiv v jednotlivých letech realizační etapy v tis. Kč

Majetek pořízený v rámci realizační etapy zůstane beze změny po celou dobu udržitelnosti projektu. Majetek bude odepisován v souladu s platnou legislativou, kde budou odpisy pouze vyjadřovat opotřebení majetku, ale nebudou mít vliv na cash flow.

Krytí majetku bude zajištěno z rozpočtu Pardubického kraje (10%), ze státního rozpočtu (5%) a z dotace IROP (85%).

- Investiční dlouhodobý majetek bude pořízen postupně v průběhu realizační fáze projektu.
- Investiční majetek bude pořízen na základě výběrových řízení, ve kterém budou vybráni nejvhodnější dodavatelé. Preferována bude nejnižší cenová nabídka, splňující požadované technické parametry specifikované v kapitole **18**.

11.1.1. majetek movitý

V rámci realizace bude pořízen dlouhodobý hmotný (movitý), který bude ve vlastnictví žadatele. Jedná se o HW, který je přehledně vidět v podkapitole 12.1.1. Dle předběžného odhadu bude pořizovací hodnota technického a technologického řešení činit zhruba 44,9 milionu Kč. Náklady budou kryty z rozpočtu projektu.

11.1.2. majetek nemovitý

V rámci projektu nebude pořizován nemovitý majetek.

11.1.3. majetek nehmotný

V rámci realizace bude pořízen nehmotný majetek, který bude ve vlastnictví žadatele. Jedná se o SW, který je přehledně vidět v podkapitole 12.1.1. Dle předběžného odhadu bude pořizovací hodnota licencí činit zhruba 5,4 milionu Kč. Náklady budou kryty z rozpočtu projektu.

11.1.4. majetek vlastní

V rámci projektu nebude pořizován majetek vlastní.

11.1.5. majetek najatý (včetně popisu cílového stavu)

V rámci projektu nebude pořizován najatý majetek.

11.1.6. majetek vypůjčený (včetně popisu cílového stavu).

V rámci projektu nebude pořizován majetek vypůjčený.

11.2. Plán investičních výdajů v realizační a provozní fázi projektu

11.2.1. Investiční dlouhodobý majetek, např. technické zhodnocení, dlouhodobý hmotný majetek (pozemek, stavba, movitá věc) nebo nehmotný majetek

Všechny majetkové položky jsou dlouhodobý hmotný nebo nehmotný majetek a nemají přesah opatření, což je z hlediska Výzvy č. 10 způsobilý výdaj. Jejich životnost je stanovena výrobci minimálně na celou dobu udržitelnosti, což je 5 let. Po dobu 5 let se nepředpokládá obnova pořízeného majetku. V tabulce níže jsou pouze výdaje na hlavní aktivity projektu.

V provozní fázi (po dobu udržitelnosti) se nepředpokládají investiční výdaje, protože životnost pořizované technologie je delší než doba udržitelnosti, případné opravy budou realizovány v rámci záruky, příp. nákupu servisních služeb a nepředpokládá se, že případné další opravy budou investičního charakteru (nepředpokládají se reinvestice).

Předpokládaná pořizovací hodnota pořizovaného majetku a odhad výdajů na pořízení tohoto majetku jsou dány rozpočtem a vyplývají z průzkumu trhu.

kód položky MS2014+	položka rozpočtu MS2014+	položka rozpočtu	jednotka	počet jednotek	Cena za jednotku	Celková cena za položku	ID technického opatření	KII/VIS/ISZS/IS/KS
1.1.1.1	Pořízení majetku	dlouhodobý hmotný a nehmotný majetek celkem	ks	18	-	50 306 614		
1.1.1.1.3.1.	Pořízení dlouhodobého hmotného majetku	Zajištění redundance optických tras pro přístupové switche	ks	1	1 573 000	1 573 000	3	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty

1.1.1.1.3.2.	Pořízení dlouhodobého hmotného maje ku	Implementace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management	ks	1	1 754 500	1 754 500	18	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.3.3.	Pořízení dlouhodobého hmotného maje ku	Doplnění redundantní [redacted]proxy	ks	1	2 635 830	2 635 830	10	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.3.4.	Pořízení dlouhodobého hmotného maje ku	Rozšíření [redacted] o SANDBOX	ks	1	4 598 000	4 598 000	11	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.3.5.	Pořízení dlouhodobého hmotného maje ku	Implementace Webového aplikačního firewallu a Loadbalanceru	ks	1	2 583 350	2 583 350	12	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.3.6.	Pořízení dlouhodobého hmotného maje ku	Implementace VPN brány	ks	1	342 558	342 558	2	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, GIS mapové servery, ISZR kukátko KS -Emailový systém
1.1.1.1.3.7.	Pořízení dlouhodobého hmotného maje ku	Vícefaktorové ověřování iden ity uživatelů a administrátorů informačních systémů	ks	1	592 295	592 295	15	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.3.8.	Pořízení dlouhodobého hmotného maje ku	Implementace řešení pro monitorování toků	ks	1	4 331 800	4 331 800	9	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty

1.1.1.1.3.9.	Pořízení dlouhodobého hmotného maje ku	Centrální logovací nástroj	ks	1	3 993 000	3 993 000	7	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.3.10.	Pořízení dlouhodobého hmotného maje ku	Doplnění HW Datového centra o servery a pole	ks	1	17 358 963	17 358 963	5	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.3.11.	Pořízení dlouhodobého hmotného maje ku	Doplnění přístupových přepínačů	ks	1	5 105 291	5 105 291	4	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.4.1.	Pořízení dlouhodobého nehmotného maje ku	Implementace testovacího centra	ks	1	121 000	121 000	17	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.4.2.	Pořízení dlouhodobého nehmotného maje ku	Implementace vysoké dostupnosti pro [redacted]	ks	1	345 606	345 606	8	VIS -Integrovaný informační systém GINIS
1.1.1.1.4.3.	Pořízení dlouhodobého nehmotného maje ku	Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě	ks	1	786 500	786 500	6	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.4.4.	Pořízení dlouhodobého nehmotného maje ku	Implementace správy privilegovaných uživatelů a účtů	Ks	1	2 359 500	2 359 500	1	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty
1.1.1.1.4.5.	Pořízení dlouhodobého nehmotného maje ku	Doplnění konektoru [redacted] pro úložiště elektronických dokumentů	ks	1	733 260	733 260	14	VIS -Integrovaný informační systém GINIS

1.1.1.1.4.6.	Pořízení dlouhodobého nehmotného maje ku	Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS	ks	1	90 750	90 750	13	VIS -Integrovaný informační systém GINIS
1.1.1.1.4.7.	Pořízení dlouhodobého nehmotného maje ku	Doplnění HW Datového centra o servery a pole	ks	1	1 001 411	1 001 411	5	VIS -Integrovaný informační systém GINIS IS - Informační systém Krajského úřadu Pardubického kraje, Webový portál Pardubického kraje, Formulářový systém sběru dat z obcí, Hostovaná spisová služba, Krajské digitální úložiště, GIS mapové servery, ISZR kukátko KS -Emailový systém, Sběrové ekonomické výkazové automaty

Tabulka 40 Vazba pořizovaného majetku na ID relevantního technického opatření – hlavní aktivity

11.2.2. Předpokládaná pořizovací hodnota majetku

V rámci realizace bude pořízen pouze dlouhodobý hmotný a nehmotný majetek, dle předběžného odhadu bude pořizovací hodnota licencí, vlastního technického a technologického řešení činit zhruba 50,3 milionu Kč.
Předpokládaná pořizovací hodnota majetku a odhad výdajů na pořízení tohoto majetku jsou dány rozpočtem a vyplývají z průzkumu trhu (viz kap. 18).

11.2.3. Výdaje na pořízení majetku

Přehled celkových nákladů v realizační fázi je uveden v kapitole 20.1 Podrobný položkový rozpočet způsobilých výdajů projektu.
Předpokládaná pořizovací hodnota majetku a odhad výdajů na pořízení tohoto majetku jsou dány rozpočtem a vyplývají z průzkumu trhu (viz kap. 18).

V realizační etapě budou kromě výdajů na pořízení dlouhodobého investičního majetku realizovány další výdaje na:

- povinnou publicitu projektu
- nákup služeb - Pořízení služeb bezprostředně souvisejících s realizací projektu

Výdaje na povinnou publicitu

- po dobu realizace projektu vystaví příjemce v místě realizace projektu na viditelném místě dočasný billboard o minimálních rozměrech 2,1 x 2,2 m
- nejpozději do tří měsíců po dokončení realizace projektu vystaví příjemce v místě jeho realizace stálou pamětní desku z odolného a trvalého materiálu a její minimální velikost by měla být 0,3 x 0,4 m
- informace na internetových stránkách

Výdaje na nákup služeb

Mezi tyto výdaje patří:

- Odborné konzultace a dozor nad implementací
- Bezpečnostní audit a penetrační testy (GAP analýza, penetrační testy)
- Výdaje na zpracování zadávacích podmínek k zakázkám a na organizaci výběrových a zadávacích řízení

Nezpůsobilé výdaje

- pojistné dlouhodobého majetku (zahrnuto v paušálním poplatku rámcové smlouvy kraje s pojišťovací společností)
- náklady na udržitelnost projektu (Údržba a servis pořízeného hmotného a nehmotného majetku)

11.2.4. Životnost majetku

Všechny majetkové položky jsou dlouhodobý investiční majetek a nemají přesah opatření, což je z hlediska Výzvy č. 10 způsobilý výdaj. Jejich životnost je stanovena výrobci minimálně na celou dobu udržitelnosti, což je 5 let. V rámci provozní fáze a doby udržitelnosti budou vynakládány provozní výdaje na servis a údržbu, Je zde ovšem možnost, že s vyšší náročností provozu bude žadatel zvažovat navýšení počtu pracovníků. Po ukončení fáze udržitelnosti předpokládáme, že na tento projekt navážou další projekty kraje dle platné legislativy, která se v oblasti kybernetické bezpečnosti může zásadním způsobem změnit. Potřebné prostředky budou naplánovány v rozpočtu kraje.

To, že se položky majetku řadí do více KII/VIS/ISZS/IS/KS nebo je jí zajišťováno více opatření, žadatel uvádí v Tabulce č. 38.

11.2.5. Převod nebo prodej majetku ve vlastnictví příjemce třetím osobám a partnerům, předpokládané termíny změn vlastnictví

V rámci projektu nebude prováděn převod nebo prodej majetku ve vlastnictví příjemce třetím osobám a partnerům.

11.2.6. Pronájem majetku třetím osobám, předpokládané termíny změn.

V rámci projektu nebude prováděn pronájem majetku třetím osobám.

11.3. Pojištění majetku

Investiční majetek, který vznikne na základě projektu, bude pojištěn proti zcizení, zničení a poškození. Náklady na pojištění jsou zahrnuty ve stávající rámcové smlouvě o pojištění majetku, kterou má Pardubický kraj uzavřenou se stávající dodavatelskou pojišťovací společností a nebudou zahrnuty do projektu.

12. Výstupy projektu

12.1. Přehled výstupů projektu a jejich kvantifikace

12.1.1. Definovaný výstup projektu

Výstupem projektu budou nové služby, hardware a software.

Položka rozpočtu	*Kvantifikace výstupů*
Opatření č. 1 - Implementace správy privilegovaných uživatelů a účtů	Interní ICT služba (SW) pro správu administrátorských účtů a účtů 3. stran.
Opatření č. 2 - Implementace VPN brány	2 ks firewallů
Opatření č. 3 - Zajištění redundance optických tras pro přístupové switche	Optické kabely + optické vany a patchpanely
Opatření č. 4 – Doplnění přístupových přepínačů	26 ks přístupových přepínačů
Opatření č. 5 - Doplnění HW Datového centra o servery a pole	HW a SW v Datacentrech
Opatření č. 6 – Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě	Interní služba (SW) pro provoz a zabezpečení IEEE802.1x
Opatření č. 7 – Centrální logovací nástroj	1 ks HW,SW
Opatření č. 8 - Implementace vysoké dostupnosti pro [redacted]	Konfigurační úpravy a SW skript pro zajištění redundantního řešení DB systému [redacted]
Opatření č. 9 - Implementace řešení pro monitorování toků	2 ks HW sonda, 2 ks HW kolektor, 1 ks SW systému pro detekci kb. událostí
Opatření č. 10 – Doplnění redundantní [redacted] proxy	1 ks appliance pro kontrolu webového provozu všech uživatelů
Opatření č. 11 – Rozšíření [redacted] o SANDBOX	2 ks appliance jako nadstavba nad řešení opatření 12 pro kontrolu webového provozu před škodlivým kódem
Opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru	2, nebo 4 boxy aplikačního FW a Loadbalanceru
Opatření č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS	SW modul do významného informačního systému GINIS, který zajistí plné zaznamenávání činností uživatelů a administrátorů v rozsahu požadovaném ZKB
Opatření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů	SW modul pro zabezpečené ukládání dat z významného informačního systému GINIS do garantovaného úložiště [redacted] v DPL2
Opatření č. 15 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů	410 ks USB čteček čipových karet + 200 čipových karet, nová služba
Opatření č. 16 – Rozšíření stávajícího dohledového centra [redacted]	Zkvalitnění stávající interní ICT služby pro monitoring infrastruktury [redacted] a zvýšení její dostupnosti

Opatření č. 17 - Implementace testovacího centra	Nový SW pro zajištění informací o akcích prováděných aplikacemi při instalacích a následném provozu
Opatření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management	Nový SW nástroj pro detekci zranitelnosti podpůrných technických aktiv a provádění bezpečnostních testů

Tabulka 41 Kvantifikace výstupů

12.1.2. Průkazné doložení a termín splnění cílů projektu a monitorovacích indikátorů

Cíle projektu bude dosaženo dle Harmonogramu dne 22.11.2019, kdy dojde k ukončení projektu k uvedení do provozu a předání do užívání. Dosažení monitorovacího indikátoru bude doloženo realizovanými technickými opatřeními. Monitorovací indikátor bude shodně naplněn dne 22.11.2019, k datu ukončení realizace projektu.

Realizace projektu bude rozdělena na implementační části. Ukončení realizace projektu bude ke dni 22.11.2019, kdy budou prokazatelně uzavřeny všechny aktivity projektu popsané již v předchozích kapitolách této studie.

Ukončení realizace projektu, tedy uzavření všech aktivit projektu, bude doloženo:

- Akceptačním protokolem o předání a převzetí díla
- Předáním do testovacího provozu
- Dodacím listem o dodání HW a SW

Ukončení realizace projektu bude, kromě výše uvedených vlastních výstupů projektu, doloženo také fotodokumentací.

Datum podepsání protokolu o předání a převzetí díla a odstranění vad a nedodělků bránících užívání díla nepřekročí termín ukončení realizace projektu uvedený v právním aktu, tj. Rozhodnutí o poskytnutí dotace (dále jen „Rozhodnutí“).

12.2. Monitorovací indikátory

12.2.1. Stanovení počáteční a cílové hodnoty monitorovacích indikátorů

Na konci projektu bude naplněn indikátor 30400 Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti, který byl žadatelem stanoven podle 10. výzvy IROP a podle pokynů v Metodickém listě indikátoru – příloha č. 5 Specifických pravidel. Tento indikátor uvádí počet realizovaných technických bezpečnostních opatření podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, jimiž je řešena kybernetická bezpečnost informačních a komunikačních systémů Pardubického kraje.

Výchozí hodnota indikátoru bude nulová v souladu s Metodickým listem indikátoru (viz příloha č. 5 Specifických pravidel).

Cílová hodnota indikátoru bude tedy 148 a bude zahrnovat počet nových nebo modernizovaných prvků zavedených u VIS/ISZS/IS/KS k zajištění standardu kybernetické bezpečnosti.

Žadatel v žádosti o podporu vyplňuje cílovou hodnotu a datum, ke kterému se zavazuje ji naplnit. K naplnění cílové hodnoty indikátoru musí dojít nejpozději k datu ukončení realizace projektu, tedy ke dni 22.11.2019. V rámci výzvy č. 10 je příjemce po celou dobu udržitelnosti zároveň povinen:

- udržet indikátory a zachovat výsledky projektu, tzn. prvky zabezpečení,

- zajistit, aby pořízené prvky kybernetické bezpečnosti sloužily svému účelu, zejména se zohledněním maximálně přípustné doby odstávky systému či akceptovatelného výpadku,
- zajistit financování veškerých výdajů spojených s provozem a údržbou pořízených prvků kybernetické bezpečnosti.

Výpočet cílové hodnoty

Prvek = technické opatření podle § 5, odst. 3, zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
Každý prvek bude do hodnoty indikátoru započítán takto:

a) V případě VIS/ISZS/IS/KS bude každý prvek započítán pro každý systém zvlášť.

b) V případě KII bude prvek započítán pouze jednou pro každou infrastrukturu, bez ohledu na to kolik jednotlivých systémů obsahuje.

Pokud bude technické opatření sdíleno více KII/VIS/ISZS/IS/KS, bude započítán tolikrát, kolika KII/VIS/ISZS/IS/KS bude sdílen.

Modernizovaným prvkem se rozumí náhrada existujícího technického opatření, které není v souladu s technickými opatřeními definovanými v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, za takové technické opatření, které je v souladu s definovanými technickými opatřeními v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti.

Výpočet:

Jelikož má žadatel definovány pouze VIS, IS a KS, cílová hodnota je počítána součinem prvku a počtu VIS, IS a KS:

Technické opatření (prvek)	počet VIS/IS/KS
Opatření č. 1 - Implementace správy privilegovaných uživatelů a účtů	**10**
Opatření č. 2 - Implementace VPN brány	**10**
Opatření č. 3 - Zajištění redundance optických tras pro přístupové switche	**10**
Opatření č. 4 – Doplnění přístupových přepínačů	**10**
Opatření č. 5 - Doplnění HW Datového centra o servery a pole	**10**
Opatření č. 6 – Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě	**10**
Opatření č. 7 – Centrální logovací nástroj	**10**
Opatření č. 8 - Implementace vysoké dostupnosti pro [redacted]	**1**
Opatření č. 9 - Implementace řešení pro monitorování toků	**10**
Opatření č. 10 – Doplnění redundantní [redacted] proxy	**10**

Opatření č. 11 – Rozšíření [redacted] o SANDBOX	**10**
Opatření č. 12 - Implementace Webového aplikačního firewallu a Loadbalanceru	**10**
Opatření č. 13 – Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS	**1**
Opatření č. 14 – Doplnění konektoru [redacted] pro úložiště elektronických dokumentů	**1**
Opatření č. 15 – Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů	**5**
Opatření č. 16 – Rozšíření stávajícího dohledového centra [redacted]	**10**
Opatření č. 17 - Implementace testovacího centra	**10**
Opatření č. 18 - Implemenace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management	**10**
Součet součinů prvků = indikátor	**148**

Tabulka 42 Výpočet cílové hodnoty Indikátoru výstupu

V následující tabulce uvádíme výchozí a cílovou hodnotu monitorovacího indikátoru.

Kód nár. číselníku	Indikátor	Měrná jednotka	Výchozí hodnota	Cílová hodnota
3 04 00	**Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti**	Počet	0	148

Tabulka 43 Indikátor výstupu a jejich kvantifikace

12.2.2. Způsob plnění monitorovacích indikátorů a jejich a vykazování

Výchozí a cílovou hodnotu, stanovenou na základě uvedených informací, žadatel zadá do žádosti o podporu v systému MS2014+.

Dosažené hodnoty vykazuje v systému MS2014+ prostřednictvím:

- Průběžných zpráv o realizaci projektu
- Závěrečné zprávy o realizaci projektu
- Zpráv o udržitelnosti projektu

Monitorovací indikátory budou doloženy:

- protokolem o předání a převzetí díla (pořízení SW/HW),
- akceptačním protokolem (předání služby)

12.3. Očekávané významné multiplikační efekty projektu (např. nepřímo vytvořená pracovní místa nebo poptávka), jejich kvantifikovaný odhad.

Neočekávají se žádné multiplikační efekty jako jsou vytváření pracovních míst (přímo ani nepřímo) nebo poptávka, projekt svým zaměřením slouží k vyšší bezpečnosti již provozovaných systémů ICT.

13. Připravenost projektu k realizaci

13.1. Technická připravenost

13.1.1. Majetkoprávní vztahy

Projekt bude realizován na pozemcích, které jsou ve vlastnictví žadatele o podporu, Pardubického kraje.

13.1.2. Připravenost projektové dokumentace

Projektem nejsou řešeny stavební úpravy, takže tato podkapitola není relevantní.

13.1.3. Připravenost dokumentace k zadávacím a výběrovým řízením, údaje o proběhlých řízeních

V rámci projektu je ukončeno VŘ na dodavatele Studie proveditelnosti. Jinak vzhledem k plánované realizaci výběrových řízení až v druhé polovině roku 2017 bude příprava dokumentace k zadávacím a výběrovým řízením teprve zahájena.
Jsou vedena dle Zákona č. 134/2016 Sb., čili Zákona o zadávání veřejných zakázek. Výčet všech VŘ následuje:

Číslo: 1

Název VŘ: Poskytování právních služeb při přípravě zadávací dokumentace a administraci zadávacích řízení
Předmět VŘ: Předmětem veřejné zakázky je uzavření smlouvy na poskytování právních službepři přípravě zadávací dokumentace a administraci zadávacích řízení dle zákona č. 134/2016 Sb. o veřejných zakázkách, ve znění pozdějších předpisů

Smluvní strana: bude vybrána
Předpokládaná hodnota: 413 223,- Kč bez DPH a 500 000,- Kč včetně DPH
Datum vyhlášení: 12.3.2018 – 19.3.2018
Z toho náklady způsobilé: 100%

Číslo: 2

Název VŘ: Objednávka odborných konzultací a dozoru nad implementací
Předmět VŘ: Předmětem veřejné zakázky je uzavření objednávky na zajištění odborných konzultací a dozoru nad implementací
Smluvní strana: bude vybrána
Smluvní hodnota: 413 223,- Kč bez DPH a 500 000,- Kč včetně DPH
Datum uzavření objednávky: v rámci 2. kvartálu 2018
Z toho náklady způsobilé: 100%

Číslo: 3

Název VŘ: Dodávka a implementace bezpečnostního projektu
Předmět VŘ: Předmětem veřejné zakázky je uzavření smlouvy na dodávku a implementaci bezpečnostního

projektu

Smluvní strana: bude vybrána

Předpokládaná hodnota: 41 575 714,- Kč bez DPH a 50 306 614,- Kč včetně DPH

Datum vyhlášení: 7.5.2018 - 5.08.2018

Z toho náklady způsobilé: 100%

Číslo: 4

Název VŘ: Provedení penetračních testů

Předmět VŘ: Předmětem veřejné zakázky je uzavření objednávky na zajištění penetračních testů

Smluvní strana: bude vybrána

Smluvní hodnota: 413 223,- Kč bez DPH a 500 000,- Kč včetně DPH

Datum uzavření objednávky: v rámci 3. kvartálu 2019

Z toho náklady způsobilé: 100%

Číslo: 5

Název VŘ: VŘ na zajištění povinné publicity.

Předmět VŘ: Předmětem veřejné zakázky je uzavření objednávky na zajištění povinné publicity

Smluvní strana: bude vybrána

Smluvní hodnota: 14 132,- Kč bez DPH a 17 100,- Kč včetně DPH

Datum uzavření objednávky: v rámci 3. kvartálu 2019

Z toho náklady způsobilé: 100%

13.2. Organizační připravenost

13.2.1. Popis procesů – organizace, odpovědnost, schvalování a kontrola v jednotlivých fázích realizace projektu (přípravná, realizační, provozní)

Pro přípravnou fázi projektu – organizace, odpovědnost, schvalování a kontrola

Pro přípravu projektu byl vytvořen projektový tým, jehož členové měli podle svých zkušeností a pracovní náplně přiřazenu funkci, roli v týmu, za kterou nesou zodpovědnost osobě, která je v hierarchii týmu pověřena schvalováním a kontrolou nad přípravou projektu a podáním žádosti o podporu do IROP.

Vedoucím projektového týmu, který má již od přípravy projektu nejvyšší odpovědnost a kompetence - schvalovací a kontrolní, je vedoucí oddělení informatiky Krajského úřadu Pardubického kraje. Má pravomoc provádět kontrolu nad činností ostatních členů týmu a dále má oprávnění schvalovat postupy přípravy projektu. Složení celého projektového týmu (vč. odpovědnosti jednotlivých členů) v přípravné fázi předkládaného projektu je v kap. 7 této studie a je také stručněji uvedeno v elektronické žádosti MS2014+.

Projektový tým se v přípravné fázi projektu scházel podle potřeby, min. však jednou za 14 dnů, a to v rámci jednání, konzultací, pochůzek v terénu i kontrolních dnů. V průběhu přípravné fáze projektu probíhala neustálá komunikace mezi jednotlivými členy týmu i konzultace s CRR, vše za účelem zajištění bezproblémové přípravy a podání žádosti o podporu z IROP.

Pro realizační fázi projektu – organizace, odpovědnost, schvalování a kontrola

Projektový tým se v realizační fázi projektu bude scházet např. v rámci kontrolních dnů na místě realizace, které budou probíhat v pravidelných časových intervalech. Těchto kontrolních dnů se budou dále účastnit zástupci dodavatele a žadatele. První kontrolní den se uskuteční při předání podkladů pro 1.implementační části projektu. Další kontrolní dny budou stanoveny na těchto pravidelných kontrolních dnech. Závěrečný kontrolní den bude spojen s prohlídkou místa realizace a dodaného díla před podpisem akceptačního protokolu před uvedením do testovacího/ostrého provozu. Členové projektového týmu se budou také scházet za účelem přípravy podkladů a zpracování zpráv o realizaci projektu, zjednodušených žádostí o platbu či závěrečné zprávy o realizaci projektu. Všichni členové týmu budou v neustálém kontaktu, dle potřeby budou vzájemně komunikovat a zodpovídají se vedoucímu projektového týmu.

Složení celého projektového týmu (vč. odpovědnosti jednotlivých členů) v realizační fázi předkládaného projektu je v kap. 7 této a je také stručněji uvedeno v elektronické žádosti MS2014+.

Pro provozní fázi projektu – organizace, odpovědnost, schvalování a kontrola

Projektový tým se v provozní fázi projektu bude scházet např. v rámci kontrolních dnů na místě provozu, které budou probíhat v pravidelných časových intervalech. Těchto kontrolních dnů se budou dále účastnit zástupci dodavatele, žadatele. První kontrolní den se uskuteční při předání podkladů pro provoz. Další kontrolní dny budou stanoveny na těchto pravidelných kontrolních dnech. Členové projektového týmu se budou také scházet za účelem přípravy podkladů a zpracování zpráv o udržitelnosti projektu. Všichni členové týmu budou v neustálém kontaktu, dle potřeby budou vzájemně komunikovat a zodpovídají se vedoucímu projektového týmu.

Složení celého projektového týmu (vč. odpovědnosti jednotlivých členů) v realizační fázi předkládaného projektu je v kap. 7 této a je také stručněji uvedeno v elektronické žádosti MS2014+.

13.3. Plán zdrojů financování

13.3.1. Způsob financování realizace projektu, včetně popisu procesu zajištění předfinancování a spolufinancování projektu,

Zdrojem financování projektu jsou Evropské strukturální a investiční fondy (Evropský fond pro regionální rozvoj – EFRR) *prostřednictvím programu Integrovaný regionální operační program, SC 3.2.* Žadateli bude v případě podpoření projektu uhrazeno z Evropských strukturálních a investičních fondů 85 % způsobilých výdajů projektu a ze státního rozpočtu 5 %. Vlastní podíl žadatele bude tvořit 10 % způsobilých výdajů. Předfinancování i spolufinancování projektu bude zajištěno v době realizace z vlastních zdrojů žadatele.

13.3.2. Zajištění financí v provozní fázi projektu

Zdrojem pro zajištění financí v provozní fázi projektu bude rozpočet Pardubického kraje.

14. Plán údržby

Implementace technických opatření implementovaných v rámci tohoto projektu vyžaduje minimálně po dobu udržitelnosti finanční a lidské investice spojené s náklady na jejich údržbu a podporu.
Předpokladem řádného provozu a naplnění požadavků zákona je proto pravidelný servis implementovaných zařízení, který obsahuje garantovanou výměnu HW v dostatečné úrovni SLA, instalaci SW aktualizací, patchů a řešení vážných provozních závad HW a SW, správu provozu, profylaxe HW/SW nebo proaktivní monitoring 24x7. Samozřejmostí je tedy řádně zakoupená podpora výrobce implementovaných zařízení včetně všech licencí nejméně po dobu udržitelnosti projektu.
Vhodné je též počítat se službami konzultací rozvojových plánu a řešení požadavků na změnu sítě, aby nedošlo k narušení funkčnosti technických opatření a předešlo se případným porušením pravidel daných výzvou 10.
Stejnou měrou je potřeba počítat s aktualizací bezpečnostních a provozních znalostí obsluhujícího personálu na straně Pardubického kraje.

14.1. Činnosti a služby spojenými s údržbou a podporou

- Poskytnutí služby garantované výměnu HW dílů za nové v případě poruchy
  - výjezd technika na místo závady
  - troubleshooting (ověření závady specialistou na danou technologickou oblast)
  - dodání náhradního dílu z vlastního servisního skladu
  - výměna a zprovoznění nového HW
  - administrace výměny vadného HW směrem k výrobci
  - zajištění reklamace vadného kusu u výrobce
- Poskytnutí systémové a konzultační podpory s reakční dobou 4 hodiny onsite
- Poskytnutí hot-line 24x7 pro nahlášení závady – telefonicky, emailem nebo přes web
- Poskytnutí profylaktické podpory

14.2. Udržitelnost

Jedná se o plnění/udržení aktivit projektu a **udržení výsledků** projektu i po jeho ukončení, resp. po skončení financování. Požadavky na udržitelnost projektů stanovuje poskytovatel dotace ve **Výzvě** k předkládání žádostí individuálních projektů ostatních
Udržitelnost může být stanovena na dobu **max. 5 let** po skončení financování projektu z OP VK - přesná doba udržitelnosti pro daný projekt je uvedena v **Rozhodnutí o poskytnutí dotace nebo-li právním aktu.**
Udržitelnost se dokládá standardním způsobem tak, jak probíhalo prokazování realizace aktivit v době realizace projektu v monitorovacích zprávách
Příjemce v době udržitelnosti předkládá dle charakteru projektu a aktivit/výstupů např. prezenční listiny, fotodokumentaci, pozvánky na semináře, programy akcí, zápisy z realizovaných cest, rozvrhy hodin/přednášek, aktualizované studijní/učební materiály, třídní knihy, výpisy z evidence majetku (pro majetek pořízený z dotace), pracovní smlouvy apod.

Příjemce nemá povinnost předkládání účetních dokladů.

Udržitelnost je doba, po kterou příjemce musí zachovat výstupy projektu v souladu s čl. 71 obecného nařízení. K udržení výstupů je příjemce zavázán v Podmínkách Stanovení výdajů či Podmínkách Rozhodnutí.

Doba udržitelnosti je stanovená na pět let od provedení poslední platby příjemci ze strany ŘO IROP, tzn. od data nastavení centrálního stavu „Projekt finančně ukončen ze strany ŘO“ v MS2014+. U příjemců typu OSS a PO OSS bude stav nastaven po schválení závěrečné ŽoP ve 2. stupni. O zahájení doby udržitelnosti je příjemce informován CRR.

Základní povinnosti příjemce jsou uvedeny v kap. 20 Obecných pravidel.

V rámci výzvy č. 10 je příjemce po celou dobu udržitelnosti zároveň povinen:

- udržet indikátory a zachovat výsledky projektu, tzn. prvky zabezpečení,
- zajistit, aby pořízené prvky kybernetické bezpečnosti sloužily svému účelu, zejména se zohledněním maximálně přípustné doby odstávky systému či akceptovatelného výpadku,
- zajistit financování veškerých výdajů spojených s provozem a údržbou pořízených prvků kybernetické bezpečnosti.

15. Analýza a řízení rizik

Cílem této kapitoly je identifikovat rizika, popsat je a eliminovat a tím zvýšit pravděpodobnost úspěchu realizace projektu.

Rizika mohou významně ovlivnit očekávané výsledky projektu. Řízení rizik je soustavná systematická činnost, která má za úkol včas zjišťovat, vyhodnocovat a minimalizovat veškerá rizika vznikající v souvislosti s realizací projektu. Smyslem řízení rizik je zvolení vhodné a efektivní taktiky či nástrojů, které napomáhají k odstranění, zmírnění nebo předcházení identifikovaných rizik. Tím je zvýšena pravděpodobnost úspěchu realizace projektu a minimalizována hrozící nebezpečí problémového průběhu.

Při zpracování identifikace rizik se vycházelo z místních znalostí a byly využity zkušenosti žadatele a zpracovatele studie proveditelnosti a zpracovatele žádosti o podporu. Součástí procesu řízení rizik je analýza rizik vztahujících se k projektu. Na identifikaci rizik projektu spolupracovali žadatel o podporu – Pardubický kraj, zpracovatel studie proveditelnosti a zpracovatel žádosti o podporu, přičemž byla využita také znalost místních poměrů žadatele i ostatních zpracovatelů.

Veškerá identifikovaná rizika projektu „název projektu" jsou i přes svoji kritičnost, a zároveň pravděpodobnost výskytu, plně žadatelem (investorem) akceptována. Žadatel přijme pro snížení rizikovosti příslušná opatření uvedená u každého typu rizika. V níže uvedené tabulce nejsou vypsána všechna technická rizika, která jsme identifikovali. Tato speciální rizika, která se týkají realizace technických opatření naleznete v kapitole 5.1.

Druh rizika a fáze projektu, ve které je možné riziko očekávat	**Závažnost rizika (1 – nejnižší, 5 – nejvyšší)**	**Pravděpodobnost výskytu/četnost výskytu rizika**	**Předcházení/eliminace rizika**
Technická rizika			
Nedostatky v projektové dokumentaci	3	2	Zajištění kvalifikovaných pracovníků s dostatečnou kapacitou, nebo nasmlouvání odboných externích zdrojů pro přípravu projektové dokumentace.
Dodatečné změny požadavků investora	3	1	Zapracování nových požadavků navýší náročnost na lidské zdroje
Výběr nekvalitního dodavatele	4	3	Kvalitně zpracovaná zadávací dokumentace a dobře volená hodnotící kritéria veřejné zakázky. Výběr prověřeného dodavatele s dostatečnými referencemi v dané oblasti. Důsledné projektové řízení umožňující včasné zjištění případných problémů.
Nedodržené termínu realizace	3	3	Kvalitní vedení projektu dle obvyklých metodik (např. PRINCE2, ..). Vhodné plánování souběhu aktivit s ohledem na interní zdroje

			žadatele, stanovení priorit a cílů fází, kontrola plnění termínů.
Zvýšení cen vstupů	3	3	Dobře vypracovaná zadávací dokumentace a kvalitní výběr dodavatele, dostatečné právní zajištění smluv a kontrola jejich dodržování.
Nedostatečná koordinace programátorských prací	3	3	Dobře vypracovaný projektový management a kontrola termínů a splněných úkolů, dostatečné právní zajištění smluv a kontrola jejich dodržování.
Živelné pohromy	1	1	Pojištění proti živelným pohromám.
Nekvalitní projektový tým	2	3	Včasné zajištění kvalifikovaných zdrojů a vyčlenění dostatečných kapacit na straně dodavatele i žadatele, vhodný výběr projektového manažera se znalostmi oblastní problematiky. Kvalitní vedení projektu dle obvyklých metodik (např PRINCE2, ..). Dostatečná motivace všech členů týmu a správné nastavení odpovědnosti.
Finanční rizika			
Neobdržení dotace	5	2	Studie a následné kroky (zadání veřejné zakázky, ...) musí být připravovány plně v souladu s požadavky a výzvy č. 10 a legislativy ČR a EU.
Nedostatek finančních prostředků na předfinancování a v průběhu realizace projektu	4	2	Dobře připravený rozsah projektu a kvalitně zpracovaná projektová dokumentace, reálně připravený cash-flow projektu, s předem potvrzeným zajištěním financování. Pravidelné vyhodnocování stavu projektu, čerpání zdrojů a reakce na změny.
Právní rizika			
Nedodržení pokynů pro zadávání VZ	3	1	Kvalitně zpracovaná zadávací dokumentace a dobře volená hodnotící kritéria veřejné zakázky. Dobře zajištěný právní servis v rámci přípravy veřejné zakázky.
Nedodržení podmínek IROP	3	1	Dobře zpracované analýzy a přehledná specifikace projektu minimalizující možnost nesouladu s podmínkami zadání.
Nedodržení právních norem ČR, EU	3	1	Kontrola všech norem v průběhu plnění.
Nevyřešené vlastnické vztahy	3	1	Dostatečné právní zajištění smluv a kontrola jejich dodržování. Vhodně volené sankční podmínky.

Provozní rizika			
Nedostatečné využití vybudovaných technických opatření	**4**	1	Monitoring dle projektu a dodržení technických parametrů a všech podmínek poskytnuté dotace
Nedostatečné personální zajištění	**4**	1	Včasné kontroly a další personální zajištění při dodržení technických parametrů a všech podmínek poskytnuté dotace
Neplnění dodavatelských smluv	3	1	Dostatečné právní zajištění smluv a kontrola jejich dodržování. Vhodně volené sankční podmínky.
Nedodržení indikátorů	**5**	1	KO kritérium pro poskytnutí dotace
Nedostatek finančních prostředků v provozní fázi projektu	3	5	Včasné zajištění finančních prostředků z rozpočtu kraje

Tabulka 44 Analýza rizik

15.1. Vyhodnocení rizik

- vyhodnocení vlivu hlavních rizik na realizaci a provoz projektu,
- návrhy opatření pro eliminaci rizik.

Z hlediska dosažené významnosti je za výrazná třeba považovat rizika přesahující svou dosaženou výší hodnotu 3 (tj. rizika s hodnotou významnosti 4 – 5, v tabulce jsou označena tučně).

Z tohoto důvodu patří mezi nejzávažnější rizika v rámci přípravy projektu výběr nekvalitního dodavatele, nedodržení indikátoru, neobdržení dotace, neplnění dodavatelských smluv a nedostatek finančních prostředků na předfinancování a v průběhu realizace projektu. Rizika ve fázi přípravy projektu se v celé řadě případů v plné míře projeví až při jeho vlastní realizaci. Z tohoto důvodu je zde proto třeba klást důraz především na předcházení vzniku těchto rizik, neboť tato rizika mohou významným způsobem ohrozit naplnění vize a dosažení specifických cílů projektu.

Ve fázi realizace jsou nejpodstatnějšími riziky nezajištění prostředků na případné vyvolané investice či jiné nezpůsobilé náklady podmiňující realizaci projektu, které nebyly předem známy a neplnění cílů či monitorovacího indikátoru v důsledku neplnění dodavatelských smluv.

Zmírnění rizik je zabezpečeno nastavením funkčního systému implementační struktury s jednoznačně vymezenými odpovědnostmi, informačními toky a několikastupňovou kontrolou a koordinací aktivit a pravidelným monitorováním projektu jako celku, které v případě potřeby umožní relativně flexibilní reakci na vzniklý problém a jeho možné následky v projektovém i celkovém měřítku.

Ve fázi udržitelnosti projektu je jako nejvýznamnější riziko chápáno nedostatečné využití vybudovaných technických opatření a nedostatečné personální zajištění. Při vzniku daného rizika je třeba se soustředit na další personální zajištění při dodržení technických parametrů a všech podmínek poskytnuté dotace.

16. Vliv projektu na horizontální kritéria

Projekt se zaměřuje v rámci zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT k zajištění standardů kybernetické bezpečnosti a svou povahou má neutrální vliv na následující horizontální principy uvedenými v dalších kapitolách níže a jsou v souladu s přílohou č. 24 Obecných pravidel pro žadatele a příjemce.

16.1. Podpora rovných příležitostí a nediskriminace

Zapojení principů rovnosti žen a mužů a nediskriminace znamená potírání diskriminace na základě pohlaví, rasy, etnického původu, náboženského vyznání, víry, zdravotního postižení, věku či sexuální orientace. Téma rovných příležitostí se vztahuje i na další znevýhodněné skupiny, jako jsou migranti, dlouhodobě nezaměstnaní, osoby s nízkou kvalifikací, osoby z obtížně dopravně dostupných oblastí, drogově závislí, propuštění vězni, absolventi škol; souhrnně skupiny sociálně vyloučené a ohrožené sociálním vyloučením.

Žadatel při analýze projektu nezaznamenal vliv, který bude mít projekt na situaci znevýhodněných skupin. Projekt má neutrální vliv na horizontální princip podpora rovných příležitostí a nediskriminace.

16.2. Podpora rovnosti mezi muži a ženami

V IROP je brán zřetel na příspěvek podporovaných aktivit k rovnosti žen a mužů. Příjemce zajišťuje rovný přístup mužů a žen do aktivit realizovaný projektem a zajistí, aby nedocházelo k diskriminaci na základě pohlaví.

Žadatel při analýze projektu nezaznamenal vliv, který bude mít projekt na rovnost mezi muži a ženami. Projekt má neutrální vliv na horizontální princip podpora rovnosti mezi muži a ženami.

16.3. Udržitelný rozvoj

Udržitelný rozvoj je definován jako rovnováha mezi ekonomickým, sociálním a environmentálním pilířem. Součástí základních moderních principů při investování veřejných prostředků je důraz na udržitelný rozvoj území, ochranu životního prostředí, účinné a úsporné využívání zdrojů, opatření vedoucí ke zmírňování změny klimatu a poskytnutí podmínek pro odolnost proti katastrofám a předcházení rizikům.
Žadatel při analýze projektu nezaznamenal vliv, který bude mít projekt na udržitelný rozvoj. Projekt má neutrální vliv na horizontální princip udržitelný rozvoj.

17. Závěrečné hodnocení efektivity a udržitelnosti projektu

Udržitelnost je doba, po kterou musí příjemce podpory udržet výstupy projektu. Projekt musí být udržitelný po dobu 5 let od finančního ukončení realizace projektu. Začátek fáze udržitelnosti je v případě předkládaného projektu očekáván od 22.11.2019.

17.1. Shrnutí zajištění udržitelnosti projektu včetně popisu zajištění vlastnických nebo jiných práv v období udržitelnosti.

Po realizaci projektu nastává provozní fáze, která s sebou přináší tzv. dobu udržitelnosti, což je 5 let po ukončení realizace. V rámci výzvy č. 10 žadatel po celou dobu udržitelnosti udržuje indikátor a zachovává výsledky projektu, tzn. prvky zabezpečení. Musí zajistit, aby pořízené prvky kybernetické bezpečnosti sloužily svému účelu, zejména se zohledněním maximálně přípustné doby odstávky systému či akceptovatelného výpadku. Musí zajistit financování veškerých výdajů spojených s provozem a údržbou pořízených prvků kybernetické bezpečnosti.
Veškerý pořízený majetek bude příjemce podpory po dobu udržitelnosti projektu používat k účelu, ke kterému se zavázal v žádosti o podporu. Příjemce po dobu udržitelnosti projektu udrží dosažené cíle a zachová výstupy projektu uvedené níže; bude dodržovat pravidla publicity; naplňovat a udržovat indikátory; veškerý pořízený majetek bude používat k účelu, ke kterému se zavázal v žádosti o podporu; bude podávat zprávy o udržitelnosti a informovat CRR o změnách v projektu; řádně uchovávat veškerou dokumentaci a účetní doklady související s projektem, apod.
V následující tabulce uvádíme realizaci monitorovacího indikátoru:
3 04 00 Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti

Vize projektu	**Bezpečnost komunikační infrastruktury**
Cílové skupiny/Subjekty zapojené do projektu	Krajský úřad a jeho zaměstnanci, organizace kraje, města a obce, občané a podnikatelé
Přepokládané výstupy	Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti
Očekávané přínosy	Zabezpečený provoz souvisejících s výkonem veřejné správy v souladu s legislativou
Klíčové aktivity	Implementace technických opatření

Tabulka 45 Výstupy a přínosy projektu

Předpokládané výstupy:

- dovybavení potřebnými HW/SW komponenty, nebo upgrade stávajících,
- optimalizace rolí jednotlivých uživatelů ICT při zajištění agend vykonávaných žadatelem,

- zajištění úpravy ICT komponent či uceleného řešení dle procesů probíhajících v rámci působností žadatele,
- prezentace poskytovaných služeb prostřednictvím portálu, včetně integrace na Portál veřejné správy.

Očekávané přínosy: Optimálně fungující bezpečnost vnitřního systému úřadu.

17.2. Zdůvodnění potřebnosti a nutnosti realizace projektu

Na základě platné legislativy je žadatel povinen zabezpečit své systémy, a to účelně a hospodárně. To je důvodem, který vedl k tomuto projektu. Studie proveditelnosti zpracovává záměr výrazného zvýšení bezpečnosti informačních systémů krajského úřadu vycházející ze zákona č.181/2014 Sb. o kybernetické bezpečnosti. Východiskem pro zpracování studie proveditelnosti byl dokument „Strategický rámec rozvoje veřejné správy ČR pro období 2014-2020“ zpracovaný Ministerstvem vnitra, odborem strategického rozvoje a koordinace veřejné správy, a to především okruh číslo 7. Kybernetická bezpečnost.
Rada Pardubického kraje se dlouhodobě zabývá bezpečností informačních systémů Krajského úřadu a rozhodla o zpracování studie proveditelnosti pro výzvu č. 10, prioritní osa 3 - Dobrá správa území a zefektivnění veřejných institucí, specifický cíl 3.2 - Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů ICT, tedy i pro oblast kybernetické bezpečnosti Pardubického kraje.

17.3. Realizace projektu při neschválení dotace.

V případě neschválení dotace by kraj projekt realizoval z rozpočtu úřadu na rok 2018 a to v nejnutnější podobě vyžadující aktuální platnou legislativou.

17.4. Popis zajištění udržitelnosti v rozdělení na část

17.4.1. Provozní část

Udržitelnost projektu z provozního hlediska se týká především zajištění:

- Servisu
- Údržby a obnovy pořízeného HW/SW
- Vyčlenění a udržení kvalitního bezpečnostního týmu

Z technologického hlediska bude nutné zajistit pravidelnou obnovu a upgrade pořízených systémů tak, aby byly schopny poskytovat plánované služby. Na konci lhůty udržitelnosti projektu bude veškerý HW/SW na podobné úrovni jako původně nakoupený. Veškerý HW/SW zůstane v majetku žadatele po celou dobu udržitelnosti projektu. Udržitelnost projektu bude zajištěna **pravidelným servisem a údržbou** a neméně důležitým bodem udržitelnosti projektu z provozní roviny je **vyčlenění dostatečného množství kvalifikovaných pracovníků** jak ze strany krajského úřadu, tak ze strany dodavatele řešení pro zajištění provozu všech nápravných opatření.

17.4.2. Administrativní část

Projektový tým bude z hlediska následných kontrol ze strany řídícího orgánu či vnějších nezávislých kontrol včetně kontrol z EU zpracovávat na základě zajištěných podkladů Monitorovací hlášení s žádostí o platbu, Závěrečné monitorovací zprávy, Monitorovací zprávy o zajištění udržitelnosti projektu.

Pardubický kraj je připraven následovně:

1. Bude zajišťovat komunikaci s ŘO/CRR – jedná se např. o zprávy o udržitelnosti projektu, případně další korespondence a související administrativu. Pardubický kraj pro tyto činnosti zajistí vlastního pracovníka.
2. Zajistí technickou, provozní (vč. údržby, oprav a obnovy) a finanční udržitelnost projektu, tj. informačních systémů a technologií vč. veškerého vybavení. Současně s tím bude udržovat dokumentaci tak, aby bylo zřejmé, že je majetek využíván v místě a k účelu, ke kterému byl pořízen a udržovat potřebné záznamy.

V rámci managementu projektu (viz kap.7) je definována i odpovědnost za udržitelnost projektu.

V rámci udržitelnosti zajistí příjemce, že bude řádně uchovávána veškerá dokumentace a účetní doklady související s realizací projektu.

Na základě uvedeného je příjemce připraven zajistit udržitelnost i z administrativního hlediska. Udržitelnost projektu administrativně zajistí žadatel pouze vlastními silami, prostřednictvím projektového týmu. Projektový tým má již nyní k dispozici kanceláře se vším potřebným vybavením. V rámci projektu nebude tedy třeba hledat a pronajímat prostory nové, ani pořizovat počítače, telefony či další techniku

17.4.3. Finanční část

Projekt není realizován za účelem tvorby zisku a navíc ani negeneruje žádné příjmy. Jeho provozní náklady budou hrazeny z vlastních zdrojů žadatele, čímž bude zajištěna udržitelnost výsledků a výstupů projektu. Projekt má význam díky svým celospolečenským přínosům, které značně převyšují hodnotu původní investice a je tak vhodný pro podporu z IROP.

Primárním cílem projektu není generovat příjmy, ale zajistit bezpečnost systémů krajského úřadu dle Kybernetického zákona.

Jak je uvedeno ve finanční analýze, veškeré náklady na provoz, údržbu a tím i na udržitelnost tohoto projektu budou financovány z rozpočtu kraje. Při pořizování nového hardwarového i softwarového vybavení budou dodrženy všechny podmínky pro zadávání veřejných zakázek dle IROP a dle podmínek pro zadávání veřejných zakázek.

V příslušných kapitolách této studie jsou uvedeny odhadované náklady na provoz vybavení a v rámci finanční analýzy jsou tyto náklady uvedeny. Z hlediska Pardubického kraje tyto náklady nijak nevybočují z běžného rámce, informační systémy, technologie a technika generují náklady na údržbu pořízeného majetku a jeho obnovu (reprodukci), které je ze strany Pardubického kraje možné plně pokrýt.

Řešení projektu je navrženo tak, aby provozní náklady na údržbu a náklady na obnovu majetku nepřevyšovaly stávající obvyklé jednotkové provozní náklady, nebo se od nich odlišovaly jen mírně. Pardubický kraj počítá s alokací a vyčleněním příslušných finančních částek ze svého rozpočtu na zajištění udržitelnosti projektu.

V rámci udržitelnosti budou vedeny a uchovávány všechny účetní doklady související s realizací projektu v souladu s podmínkami dotace.

.

18. Způsob stanovení cen do rozpočtu projektu

18.1. Princip a výchozí informace

- Zadávací/výběrové řízení nebylo zahájeno (dále také „nezahájená zakázka"), žadatel předkládá stanovení cen do rozpočtu projektu nebo způsob stanovení předpokládané hodnoty zakázky.
- V případě přímých nákupů od 100 000 Kč bez DPH žadatel překládá stanovení cen do rozpočtu. Stanovení ceny přímých nákupů do 100 000 Kč bez DPH žadatel nepředkládá.

18.2. Způsob stanovení cen

Zpracovatel zajistil průzkum trhu u několika dodavatelů, kteří jsou uvedeni v Tabulce č. 46 Stanovení cen do Rozpočtu projektu, za účelem zjištění předpokládané ceny způsobilých výdajů hlavních aktivit projektu u nezahájených zakázek. Stanovení cen do rozpočtu ve vztahu k plánovaným hlavním aktivitám projektu je rozděleno do samostatných celků tak, aby tyto celky odpovídaly předmětům plnění všech zakázek.

Stáří zdrojových dat pro doložení ceny je do 6 měsíců před datem podání žádosti o podporu, což žadatel splňuje, protože jsou od 10.5.2017 a mladší.

Předpokládané ceny spadající do **hlavních aktivit projektu** žadatel stanovil na základě údajů a informací získaných průzkumem trhu s požadovaným plněním, kdy

- průzkum trhu byl proveden e-mailovým oslovením 4 dodavatelů nebo výrobců, kteří se poptávaným plněním skutečně zabývají či ho standardně nabízí. Až na jednoho, všichni poslali nabídku
- pouze v případě rozšíření systému GINIS byl poptán výrobce a jeho jediný distributor (Opatření č.14 a 15)
- žadatel zvolil **nejnižší nabídkovou cenu**, jejímž obsahem je celková cena bez DPH za investici včetně 5letého provozu
- Stanovení cen nákladů na vedlejší aktivity provedl žadatel kvalifikovaným odhadem.
- Žadatel má k dispozici podklady, ze kterých vycházel při stanovení cen do rozpočtu projektu (písemná či elektronická komunikace s oslovenými dodavateli). Na výzvu je připraven je doložit.

číslo podkladu	podklad ze dne	Zdroj informací	Předpokládaná hodnota VŘ/ZŘ bez DPH	Použitá cena (bez DPH) do rozpočtu	Použitá cena (včetně DPH) do rozpočtu	kód položky rozpočtu	princip stanovení ceny	VŘ č.	Plánované zahájení VŘ
Zajištění redundance optických tras pro přístupové switche									
1	10.5.2017	S&T CZ s.r.o.	1 300 000 Kč	1 300 000 Kč	1 573 000 Kč	1.1.1.1.3.1.	průzkum trhu	5	27.9.2017
2	10.5.2017	SITEL, spol. s r.o.	1 341 998 Kč						
3	10.5.2017	VERTIX s.r.o.	1 357 000 Kč						
Implementace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management									
1	10.5.2017	S&T CZ s.r.o.	1 450 000 Kč	1 450 000 Kč	1 754 500 Kč	1.1.1.1.3.2.	průzkum trhu	5	27.9.2017
2	10.5.2017	VERTIX s.r.o.	1 490 000 Kč						
3	10.5.2017	ICZ a.s.	1 540 000 Kč						
Doplnění redundantní [redacted] proxy									
1	10.5.2017	VERTIX s.r.o.	4 180 000 Kč	1 744 838 Kč	2 111 253 Kč	1.2.1.1.	průzkum trhu	5	27.9.2017
2	10.5.2017	ICZ a.s.	3 923 210 Kč	2 178 372 Kč	2 635 830 Kč	1.1.1.1.3.3.			

3	10.5.2017	S&T CZ s.r.o.	4 250 000 Kč						
Rozšíření [redacted] o SANDBOX									
1	10.5.2017	VERTIX s.r.o.	6 400 000 Kč	3 800 000 Kč	4 598 000 Kč	1.1.1.1.3.4.	průzkum trhu	5	27.9.2017
2	10.5.2017	S&T CZ s.r.o.	5 000 000 Kč	1 200 000 Kč	1 452 000 Kč	1.2.1.1.			
3	10.5.2017	ICZ a.s.	8 744 520 Kč						
Implementace Webového aplikačního firewallu a Loadbalanceru									
1	10.5.2017	VERTIX s.r.o.	6 890 000 Kč	2 135 000 Kč	2 583 350 Kč	1.1.1.1.3.5.	průzkum trhu	5	27.9.2017
2	10.5.2017	S&T CZ s.r.o.	4 025 000 Kč	1 890 000 Kč	2 286 900 Kč	1.2.1.1.			
3	10.5.2017	ICZ a.s.	9 796 892 Kč						
Implementace VPN brány									
1	10.5.2017	ICZ a.s.	386 742 Kč	283 106 Kč	342 558 Kč	1.1.1.1.3.6.	průzkum trhu	5	27.9.2017
2	10.5.2017	S&T CZ s.r.o.	600 000 Kč	103 636 Kč	125 400 Kč	1.2.1.1.			
3	10.5.2017	VERTIX s.r.o.	540 000 Kč						
Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů									
1	10.5.2017	S&T CZ s.r.o.	489 500 Kč	489 500 Kč	592 295 Kč	1.1.1.1.3.7.	průzkum trhu	5	27.9.2017
2	10.5.2017	ICZ a.s.	534 000 Kč						
3	10.5.2017	VERTIX s.r.o.	528 000 Kč						
Implementace řešení pro monitorování toků									
1	10.5.2017	ICZ a.s.	8 962 745 Kč	3 980 000 Kč	4 815 800 Kč	1.2.1.1.	průzkum trhu	5	27.9.2017
2	10.5.2017	S&T CZ s.r.o.	7 560 000 Kč	3 580 000 Kč	4 331 800 Kč	1.1.1.1.3.8.			
3	10.5.2017	VERTIX s.r.o.	8 126 000 Kč						
Centrální logovací nástroj									
1	10.5.2017	ICZ a.s.	6 619 358 Kč	3 300 000 Kč	3 993 000 Kč	1.1.1.1.3.9.	průzkum trhu	5	27.9.2017
2	10.5.2017	S&T CZ s.r.o.	5 950 000 Kč	2 650 000 Kč	3 206 500 Kč	1.2.1.1.			
3	10.5.2017	VERTIX s.r.o.	7 000 000 Kč						
Doplnění HW Datového centra o servery a pole									
1	10.5.2017	ICZ a.s.	23 292 559 Kč	14 346 250 Kč	17 358 963 Kč	1.1.1.1.3.10.	průzkum trhu	5	27.9.2017
2	10.5.2017	S&T CZ s.r.o.	17 423 048 Kč	827 612 Kč	1 001 411 Kč	1.1.1.1.4.7.			
3	10.5.2017	VERTIX s.r.o.	24 000 000 Kč	2 249 186 Kč	2 721 515 Kč	1.2.1.1.			
Doplnění přístupových přepínačů									
1	10.5.2017	VERTIX s.r.o.	5 640 000 Kč	4 219 249 Kč	5 105 291 Kč	1.1.1.1.3.11.	průzkum trhu	5	27.9.2017
2	10.5.2017	ICZ a.s.	4 899 858 Kč	680 609 Kč	823 536 Kč	1.2.1.1.			
3	10.5.2017	S&T CZ s.r.o.	8 263 084 Kč						
Implementace testovacího centra									
1	10.5.2017	ICZ a.s.	180 000 Kč	100 000 Kč	121 000 Kč	1.1.1.1.4.1.	průzkum trhu	5	27.9.2017
2	10.5.2017	S&T CZ s.r.o.	100 000 Kč						
3	10.5.2017	VERTIX s.r.o.	250 000 Kč						
Implementace správy privilegovaných uživatelů a účtů									
1	10.5.2017	S&T CZ s.r.o.	4 250 000 Kč	2 300 000 Kč	2 783 000 Kč	1.2.1.1.	průzkum trhu	5	27.9.2017
2	10.5.2017	ICZ a.s.	5 000 000 Kč	1 950 000 Kč	2 359 500 Kč	1.1.1.1.4.4.			
3	10.5.2017	VERTIX s.r.o.	5 100 000 Kč						
Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě									
1	10.5.2017	S&T CZ s.r.o.	650 000 Kč	650 000 Kč	786 500 Kč	1.1.1.1.4.3.	průzkum trhu	5	27.9.2017

2	10.5.2017	ICZ a.s.	775 000 Kč						
3	10.5.2017	VERTIX s.r.o.	870 000 Kč						
Implementace vysoké dostupnosti pro [redacted]									
1	10.5.2017	VERTIX s.r.o.	532 000 Kč	192 500 Kč	232 925 Kč	1.2.1.1.	průzkum trhu	5	27.9.2017
2	**10.5.2017**	**ICZ a.s.**	**478 125 Kč**	285 625 Kč	345 606 Kč	1.1.1.1.4.2.			
3	10.5.2017	S&T CZ s.r.o.	570 000 Kč						
Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS									
1	10.5.2017	není dodavatel		48 000 Kč	58 080 Kč	1.2.1.1.	průzkum trhu	5	27.9.2017
2	**10.5.2017**	**KMS software s.r.o.**	**123 000 Kč**	75 000 Kč	90 750 Kč	1.1.1.1.4.6.			
3	10.5.2017	GORDIC spol. s r. o.	130 500 Kč						
Doplnění konektoru [redacted] pro úložiště elektronických dokumentů									
1	10.5.2017	není dodavatel		448 800 Kč	543 048 Kč	1.2.1.1.	průzkum trhu	5	27.9.2017
2	**10.5.2017**	**KMS software s.r.o.**	**1 054 800 Kč**	606 000 Kč	733 260 Kč	1.1.1.1.4.5.			
3	10.5.2017	GORDIC spol. s r. o.	1 077 300 Kč						

Tabulka 46 Stanovení cen do Rozpočtu projektu

19. Stavební řízení

19.1. Žadatel popíše jednotlivé kroky a termíny (harmonogram) stavebního řízení.

Podkapitola není relevantní, protože předkládaným projetkem nejsou realizovány stavební práce.

19.2. V případě, že projekt nepočítá se stavebními pracemi, žadatel uvede, že se na něj nevztahuje povinnost dokládání stavebního povolení ani ohlášení.

Součástí opatření navrhovaných v rámci této studie nejsou žádné aktivity, které by si vyžadovaly stavební práce. Na žadatele se proto nevztahují povinnosti dokládání stavebního povolení ani ohlášení.

20. Finanční analýza

20.1. Podrobný položkový rozpočet způsobilých výdajů projektu – u každé položky rozpočtu projektu musí být uvedeno, zda se jedná o hlavní nebo vedlejší aktivity projektu podle kap. 2.2 Specifických pravidel a zároveň musí být uvedena konkrétní vazba na výběrové/zadávací

Finanční limity na jednotlivá technická opatření jsou v rámci projektu splněny, neboť na navrhovaných 18 technických opatření se jedná o limit cca 122 mil. Kč, který je v tomto projektu pouze cca 53 mil. Kč.

Výdaje na vedlejší aktivity projektu jsou pod 15 % celkových způsobilých výdajů, přesně se jedná o 5,13% celkových způsobilých výdajů.

Rozpočet byl stanoven na základě průzkumu trhu (kap. 18) a ze zkušeností zpracovatele studie proveditelnosti příp. žadatele o podporu s podobnými zakázkami.

Celkové způsobilé náklady projektu (v Kč)									
kód položky MS2014+	položka rozpočtu MS2014+	položka rozpočtu	jednotka	počet jednotek	Cena za jednotku	Celková cena za položku (způsobilé výdaje)	DPH 21%	hlavní/vedlejší aktivita projektu	výběrové řízení č.
1.1	Celkové způsobilé výdaje	Způsobilé výdaje celkem				53 033 714	9 204 198		
1.1.1	Celkové způsobilé výdaje - investiční	Pořízení majetku	ks		-	50 306 614	8 730 900	hlavní	
1.1.1.1	Pořízení majetku	dlouhodobý hmotný a nehmotný majetek celkem	ks	18	-	50 306 614	8 730 900	hlavní	
1.1.1.1.1	Pořízení drobného hmotného majetku	Nákup drobného hmotného	ks	0	0	0	0	hlavní	
1.1.1.1.2	Pořízení drobného nehmotného majetku	Nákup drobného nehmotného	ks	0	0	0	0	hlavní	
1.1.1.1.3	Pořízení dlouhodobého hmotného majetku	Nákup dlouhodobého hmotného celkem	ks	11	44 868 587	44 868 587	7 787 110	hlavní	
1.1.1.1.3.1.	Pořízení dlouhodobého hmotného majetku	Zajištění redundance optických tras pro přístupové switche	ks	1	1 573 000	1 573 000	273 000	hlavní	

1.1.1.1.3.2.	Pořízení dlouhodobého hmotného majetku	Implementace programového vybavení pro troubleshooting a penetrační testování - Vulnerability management	ks	1	1 754 500	1 754 500	304 500	hlavní	
1.1.1.1.3.3.	Pořízení dlouhodobého hmotného majetku	Doplnění redundantní [redacted] proxy	ks	1	2 635 830	2 635 830	457 458	hlavní	
1.1.1.1.3.4.	Pořízení dlouhodobého hmotného majetku	Rozšíření [redacted] o SANDBOX	ks	1	4 598 000	4 598 000	798 000	hlavní	
1.1.1.1.3.5.	Pořízení dlouhodobého hmotného majetku	Implementace Webového aplikačního firewallu a Loadbalanceru	ks	1	2 583 350	2 583 350	448 350	hlavní	
1.1.1.1.3.6.	Pořízení dlouhodobého hmotného majetku	Implementace VPN brány	ks	1	342 558	342 558	59 452	hlavní	
1.1.1.1.3.7.	Pořízení dlouhodobého hmotného majetku	Vícefaktorové ověřování identity uživatelů a administrátorů informačních systémů	ks	1	592 295	592 295	102 795	hlavní	
1.1.1.1.3.8.	Pořízení dlouhodobého hmotného majetku	Implementace řešení pro monitorování toků	ks	1	4 331 800	4 331 800	751 800	hlavní	
1.1.1.1.3.9.	Pořízení dlouhodobého hmotného majetku	Centrální logovací nástroj	ks	1	3 993 000	3 993 000	693 000	hlavní	
1.1.1.1.3.10.	Pořízení dlouhodobého hmotného majetku	Doplnění HW Datového centra o servery a pole	ks	1	17 358 963	17 358 963	3 012 713	hlavní	
1.1.1.1.3.11.	Pořízení dlouhodobého hmotného majetku	Doplnění přístupových přepínačů	ks	1	5 105 291	5 105 291	886 042	hlavní	
1.1.1.1.4	Pořízení dlouhodobého nehmotného majetku	Nákup dlouhodobého nehmotného celkem	ks	7	5 438 027	5 438 027	943 790	hlavní	

1.1.1.1.4.1.	Pořízení dlouhodobého nehmotného majetku	Implementace testovacího centra	ks	1	121 000	121 000	21 000	hlavní	
1.1.1.1.4.2.	Pořízení dlouhodobého nehmotného majetku	Implementace vysoké dostupnosti pro [redacted]	ks	1	345 606	345 606	59 981	hlavní	
1.1.1.1.4.3.	Pořízení dlouhodobého nehmotného majetku	Implementace řízení přístupu k síťovým prvkům a 802.1x řízení přístupu do vnitřní sítě	ks	1	786 500	786 500	136 500	hlavní	
1.1.1.1.4.4.	Pořízení dlouhodobého nehmotného majetku	Implementace správy privilegovaných uživatelů a účtů	ks	1	2 359 500	2 359 500	409 500	hlavní	
1.1.1.1.4.5.	Pořízení dlouhodobého nehmotného majetku	Doplnění konektoru [redacted] pro úložiště elektronických dokumentů	ks	1	733 260	733 260	127 260	hlavní	
1.1.1.1.4.6.	Pořízení dlouhodobého nehmotného majetku	Implementace SW pro zajištění sběru transakčních logů z jednotlivých modulů systému GINIS	ks	1	90 750	90 750	15 750	hlavní	
1.1.1.1.4.7.	Pořízení dlouhodobého nehmotného majetku	Doplnění HW Datového centra o servery a pole	ks	1	1 001 411	1 001 411	173 799	hlavní	
1.1.2	Celkové způsobilé výdaje - neinvestiční	nákup služeb a povinná publicita	ks		2 727 100	2 727 100	473 298	vedlejší	
1.1.2.1	Nákupy služeb	nákup služeb	ks	4	2 710 000	2 710 000	470 331	vedlejší	
1.1.2.1.1.	Pořízení služeb bezprostředně souvisejících s realizací projektu	výdaje na zpracování zadávacích podmínek k zakázkám a na organizaci výběrových a zadávacích řízení	ks	1	500 000	500 000	86 777	vedlejší	1.

1.1.2.1.2.	Pořízení služeb bezprostředně souvisejících s realizací projektu	Bezpečnostní audit a analýza (GAP)	ks	1	1 210 000	1 210 000	210 000	vedlejší	3.
1.1.2.1.3.	Pořízení služeb bezprostředně souvisejících s realizací projektu	Bezpečnostní audit a analýza (penetrační testy)	ks	1	500 000	500 000	86 777	vedlejší	4.
1.1.2.1.4.	Pořízení služeb bezprostředně souvisejících s realizací projektu	Odborné konzultace a dozor při implementaci	ks	1	500 000	500 000	86 777	vedlejší	2.
1.1.2.1.5.	Pořízení služeb bezprostředně souvisejících s realizací projektu	Projektová dokumentace stavebních prací a úprav	ks		0	0	0	vedlejší	-
1.1.2.1.6.	Stavební úpravy	Technický dozor investora, BOZP, autorský dozor	ks		0	0	0	vedlejší	-
1.1.2.2	Publicita projektu	Publicita projektu	ks	2	17 100	17 100	2 968	vedlejší	
1.1.2.2.1	Povinná publicita	Náklady na nákup informačních tabulí (billboard)	ks	1	5 000	5 000	868	vedlejší	5.
1.1.2.2.2	Povinná publicita	Náklady na nákup pamětních desek	ks	1	12 100	12 100	2 100	vedlejší	

Tabulka 47 Podrobný položkový rozpočet způsobilých výdajů projektu

20.2. Případné čisté jiné peněžní příjmy během realizace projektu.

Žadatel v projektu nepředpokládá jiné peněžní příjmy, tj. příjmy vytvořené v průběhu realizace projektu a vyvolané samotným projektem, nevztahuje se na něj tedy povinnost výpočtu čistých jiných peněžních příjmů dle přílohy č. 29 Obecných pravidel.

20.3. Plán cash-flow v provozní fázi projektu v členění po kalendářních letech

Finanční plán realizační a provozní fáze je totožný s výše uvedenými rozpočty, neboť projekt negeneruje příjmy a nemá další peněžně vyjádřené náklady. Po celou dobu realizační i provozní fáze jsou finanční toky plynoucí z projektu záporné, což je způsobeno nulovými příjmy projektu. Celý projekt je koncipován jako neziskový a jeho přínosy jsou nefinanční povahy.

Odpisy v realizační fázi nejsou uvedeny, protože žadatel majetek nebude odepisovat. V realizační fázi nebudou vznikat žádné výnosy. Náklady realizační fáze budou kryty z dotace evropské unie (85%), ze státního rozpočtu

(5%) a rozpočtu kraje (10%).

Provozní fáze vychází částečně z celkových nákladů realizační fáze, některé náklady jsou však kalkulovány dle skutečného odhadu. Náklady provozní fáze jsou kalkulovány na dobu udržitelnosti projektu, tzn. v délce pěti let.

V provozní fázi Projektu budou vznikat následující náklady, které jsou stanoveny na roční bázi:

Náklady na servis a údržbu – systém bude vyžadovat fungování v režimu 24x7 hodin.

V provozní fázi nebudou vznikat žádné provozní výnosy. Projekt je ze svého principu nevýdělečný, jedná se o zabezpečení systému. Veškeré provozní náklady budou hrazeny z rozpočtu žadatele.

Výnosy nejsou do peněžního toku zahrnuty, protože žádné nejsou. Finanční peněžní tok ukazuje zdroj financování provozních nákladů, tedy vlastní zdroje žadatele na bankovním účtu. Kumulované cash-flow jsou po celou dobu provozní fáze období nulové. Po dobu udržitelnosti žadatel a příjemce nepředpokládá reinvestice.

Rok	2017	2018	2019	2020	2021	2022	2023	2024 (do 22.11.)	Celkem
Investiční výdaje	0		-50 306 614	0					**-50 306 614**
Neinvestiční výdaje		-1 710 000	-1 017 100	0					**-2 727 100**
Způsobilé výdaje		-1 710 000	-51 323 714	0	0	0	0	0	**-53 033 714**
Servis a údržba (od 23.11.2019)	0	0	-352 666	-4 231 991	-4 231 991	-4 231 991	-4 231 991	-3 879 326	**-21 159 957**
Personální náklady na 1 člověka	0	0	0	0	0	0	0	0	**0**
Pojištění	0	0	0	0	0	0	0	0	**0**
Zpracování Studie proveditelnos	-301 169								
Nezpůsobilé výdaje	-301 169	0	-352 666	-4 231 991	-4 231 991	-4 231 991	-4 231 991	-3 879 326	**-21 461 126**
Výdaje celkem	**-301 169**	**-1 710 000**	**-51 676 380**	**-4 231 991**	**-4 231 991**	**-4 231 991**	**-4 231 991**	**-3 879 326**	**-74 494 840**
Příjmy Dotace EU (IROP)	0	0	0	45 078 657	0	0	0	0	**45 078 657**
Příjmy Státní rozpočet	0	0	0	2 651 686	0	0	0	0	**2 651 686**
Příjmy Národní veřejné zdroje (rozpočet kraje)	301 169,00	171 000,00	5 485 037	4 231 991	4 231 991	4 231 991	4 231 991	3 879 326	**26 764 498**
Příjmy celkem	**301 169**	**171 000**	**5 485 037**	**51 962 334**	**4 231 991**	**4 231 991**	**4 231 991**	**3 879 326**	**74 494 840**

Tabulka 48 Plán cash-flow v provozní fázi projektu v členění po kalendářních letech

20.3.1. Provozní výdaje (výdaje na údržbu) a případné příjmy příjemce plynoucí z provozu projektu, stanovené bez zohlednění inflace

Přehled celkových nákladů v provozní fázi:

- Náklady na servis a údržbu
- Mzdové náklady
- Pojištění

Položka	2019 (od 23.11.)	2020	2021	2022	2023	2024 (do 22.11.)
Servis a údržba	352 666	4 231 991	4 231 991	4 231 991	4 231 991	3 879 326
Personální náklady na 1 člověka	-	-	-	-	-	-
Pojištění	-	-	-	-	-	-
Náklady celkem	**352 666**	**4 231 991**	**4 231 991**	**4 231 991**	**4 231 991**	**3 879 326**

Tabulka 49 Odhad provozních nákladů v letech 2018 - 2024

20.3.2. Zdroje financování projektu

Projekt bude řešen v rámci finanční podpory IROP a ze spolufinancování žadatele a vychází z projektového okruhu č. 7 implementačního plánu č.3 Strategického rámce rozvoje veřejné správy, kdy výše podpory je 85 %+ 5% pro realizační část, finanční spoluúčast žadatele o podporu (kraj) je 10 %. Provozní náklady jsou 100% hrazeny žadatelem o podporu po dobu udržitelnosti projektu, což je 5 let. Následující tabulka uvádí celkovou strukturu financování projektu.

Zdroj financování	% spoluúčasti	rozsah financí v Kč (vč. DPH)
Náklady realizační fáze	100%	53 033 714 Kč
Strukturální fondy EU (IROP)	85%	45 078 657 Kč
Státní rozpočet	5%	2 651 686 Kč
Národní veřejné zdroje (rozpočet kraje)	10%	5 303 371 Kč
Finanční krytí investice	z rozpočtu kraje	53 033 714 Kč
Rozdíl	0	0 Kč
Provozní náklady (1 rok)	100%	4 231 991 Kč
Provozní náklady (5 let)	100%	21 159 957 Kč
Finanční krytí provozu (5 let)	z rozpočtu kraje	21 159 957 Kč
Rozdíl	0	0 Kč

Tabulka 50 Zdroje projektu v Kč vč. DPH

20.4. Vyhodnocení plánu cash-flow

Cash-flow a deficity jsou v rámci jednotlivých let vyrovnané. Negativní cash-flow není plánováno (pokud neplánujeme zpoždění plateb z proplácení projektu, což je v cashflow vidět) a všechny náklady jsou kompenzovány z rozpočtu kraje a dotace. Zpracovatel této studie zvolil výpočet cash-flow nepřímou metodou, která dělí cash-flow na provozní, investiční a finanční tok.

Z přehledu příjmů a výdajů realizační fáze projektu vyplývá stav finančních prostředků na konci jednotlivých období. Kumulované cash-flow je v průběhu dvou sledovaných let realizační fáze (rok 2018, 2019) záporné díky výdajům vynaloženým na pořízení služeb a majetku souvisejícího s realizací modernizace infrastruktury PK. Jeho hodnota se postupně zvyšuje v závislosti na předložených žádostech o platbu a na obdržené dotaci. Jediná žádost o platbu bude žadateli proplacena v roce 2020. Kumulovaná hodnota cash-flow je vyrovnána na nulu v roce 2020, kdy žadatel obdrží dotaci na základě žádosti o platbu.

Předfinancování a kofinancování projektu proběhne z vlastních zdrojů žadatele. Pardubický kraj tak bude projekt spolufinancovat ve výši 10 % způsobilých výdajů, a zároveň budou z žadatelova účtu hrazeny nezpůsobilé výdaje v plné výši.

Hodnocení v rámci finanční analýzy se obecně nezabývá širšími efekty projektu (celospolečenskými dopady, dopady na životní prostředí apod. na Pardubický kraj), pracuje čistě s příjmy, výdaji a cash-flow v realizační a provozní fázi projektu, jejím úkolem je prokázat zda projekt generuje takový tok peněžních prostředků, který bude moci zajistit dostatečnou rentabilitu celého projektu. Je určena především pro projekty komerčního charakteru. Po celou dobu realizační i provozní fáze jsou finanční toky plynoucí z projektu záporné, což je způsobeno nulovými příjmy projektu. Celý projekt je koncipován jako neziskový a jeho přínosy jsou nefinanční povahy.

Ztrátový provoz, který teoreticky může nastat, ovšem projekt s ním nepočítá, bude vždy krytý z prostředků žadatele, tedy z rozpočtu kraje (Národní veřejné zdroje).

Souhrnně:

1. V roce 2017 budou realizovány a žadatelem zaplaceny převážně administrativní aktivity, které budou vyúčtovány a proplaceny z dotace až v rámci vyúčtování etapy v roce 2020.
2. Aktivity budou realizovány v letech 2018-2019 a zaplaceny v letech 2018-2019 a následně vyúčtovány v rámci ukončení etapy projektu, která je plánována v roce 2019 bezprostředně po realizaci těchto aktivit.
3. **Předfinancování a spoluúčast žadatele budou realizovány z rozpočtu žadatele**, tj. negativní cash-flow na začátku projektu bude řešeno z rozpočtu žadatele.
4. Záporné částky u rozpočtu kraje znamenají příjem z proplacené dotace Evropského fondu pro regionální rozvoj a státního rozpočtu. Důvodem je, aby celkový součet částek za všechny uvedené roky odpovídal skutečnému zatížení rozpočtu žadatele.
5. Proplacení dotace bude v roce 2020.
6. Provozní výdaje budou financovány z rozpočtu žadatele, tj. Pardubického kraje.
7. Žadatel nemá nárok na odpočet DPH ve vztahu k projektu, tj. není explicitně vyčíslena DPH.

21. Přílohy

21.1. Příloha č. 1 Doplňující vyjádření ke studii na základě požadavků OHA

1. Stručný popis organizačních opatření (§5, odst. (2) ZoKB), která KÚ Pardubického kraje již realizoval nebo bude v průběhu projektu realizovat,

   KÚ Pardubického kraje jako držitel certifikátu ISO27001 již zavedl, udržuje a zlepšuje všechna organizační opatření dle ZoKB (§5, odst. (2)), tedy:

   a) systém řízení bezpečnosti informací,

   b) řízení rizik,

   c) bezpečnostní politika,

   d) organizační bezpečnost,

   e) stanovení bezpečnostních požadavků pro dodavatele,

   f) řízení aktiv,

   g) bezpečnost lidských zdrojů,

   h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,

   i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,

   j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,

   k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

   l) řízení kontinuity činností a

   m) kontrola a audit kritické informační infrastruktury a významných informačních systémů.

2. zda jsou v souladu s §6 Vyhlášky 316/2014 Sb., vyhláška o kybernetické bezpečnosti určeny bezpečnostní role manažera KB, architekta KB, auditora KB a garantů aktiv,

   Jako Orgán uvedená v § 3 písm. e) máme přiměřeně určeny bezpečnostní role.

   Máme:

   a) výbor pro řízení kybernetické bezpečnosti

   b) manažer kybernetické bezpečnosti,

   c) garanty aktiva

   Role auditor kybernetické bezpečnosti je naplňována každoročními externími audity dle požadavků ISO27001.

3. bezpečnostní požadavky pro dodavatele, kteří se budou podílet na rozvoji, provozu nebo zajištění bezpečnosti významného informačního systému dle § 7 Vyhlášky 316/2014 Sb., vyhláška o kybernetické bezpečnosti,

   Organizační opatření, stanovení bezpečnostních požadavků pro dodavatele, máme zavedeno.

   Bezpečnostní požadavky jsou stanovovány dle bezpečnostní dokumentace KÚ Pardubického kraje a následně ošetřeny ve smlouvě s dodavatelem.

   V rámci systému řízení bezpečnosti informací dále konkretizujeme a vyhodnocujeme dle našich potřeb a vývoje.

4. informaci, že projekt bude v souladu i s nově navrhovanými opatřeními (např. problematika digitální služby) uvedenými v novelizovaném ZoKB platném od 1. července 2017.

   Návrh bezpečnostních opatření, která jsou součástí studie plně reflektuje aktuální analýzu rizik krajského úřadu. Veškerá navržená technická opatření jsou plně v souladu s aktuálním zněním ZoKB a zároveň odpovídají aktuálnímu best practices. Součástí realizace projektu je i GAP analýza, která umožní reflektovat v nastavení dodávaných opatření i aktuální situaci v platné legislativě, technických a bezpečnostních standardech.