Možné projekty v IROP 2021 - 2027

Ing. Barbora Hubatková, MSc.
ICT konzultant

Oblast kybernetická bezpečnost
Povinné dokumenty

Referenční dokumenty

- Příloha žádosti – Souhlasné stanovisko Hlavního architekta eGovernmentu
- Žádost o podporu
- Studie proveditelnost

Oblast kybernetická bezpečnost
Podmínky

Specifická kritéria projektů (řešení) kybernetické bezpečnosti **jsou definována následovně**:

- Projekt je zaměřen na realizaci technických bezpečnostních opatření podle hlavy II, vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“

Hodnocení projektů kybernetické bezpečnosti (podmínky)

- projekt je zaměřen na realizaci technických bezpečnostních opatření podle hlavy II, vyhlášky o kybernetické bezpečnosti a současně je v souladu s Prováděcím dokumentem programu Digitální Česko pro čerpání z IROP 2021–2027

Technická opatření dle vyhlášky 82 ZoKB

- §17 Fyzická bezpečnost
- §18 Bezpečnost komunikačních sítí
- §19 Správa a ověřování identit
- §20 Řízeni přístupových oprávněni
- §21 Ochrana před škodlivým kódem
- §22 Zaznamenávání událostí IKS, jeho uživatelů a administrátorů
- §23 Detekce kybernetických bezpečnostních událostí
- §24 Sběr a vyhodnocování kybernetických událostí
- §25 Aplikační bezpečnost
- §26 Kryptografické prostředky
- §27 Zajišťování úrovně dostupnosti informací

Možná řešení dle vyhlášky 82 ZoKB

§ 17 Fyzická bezpečnost

- mechanické zábranné nástroje nebo prostředky (bezpečnostní systém centrálního klíče, protipožární dveře)
- nástroje elektrické zabezpečovací signalizace (PZTS - poplachový zabezpečovací a tísňový systém, EPS - elektrický (proti)požární systém, systém stabilního hasicího zařízení, aj.)
- nástroje ochrany elektrického napájení (systém elektrického napájení DR, zařízení elektrické přepěťové ochrany, záložní zdroje elektrického napájení - UPS, agregát)
- nástroje kontroly vstupu do zabezpečené oblasti (EVS - elektronicky vstupní systém s ověřením osoby)
- nástroje sledování zabezpečené oblasti (kamerový systém CCTV (Closed-circuit television), dohledový systém stavu síťových zařízení a služeb)

Možná řešení dle vyhlášky 82 ZoKB

§18 Bezpečnost komunikačních sítí

Síťové prvky a bezpečnostní prvky zajišťující:

- segmentaci sítě
- řízení komunikace (přístupu a autentizace zařízení a uživatelů v síti)
- šifrovaný vzdálený přístup k síti
- blokování (filtrování) nežádoucí komunikace

Možná řešení dle vyhlášky 82 ZoKB

§19 Správa a ověřování identit

- Bezpečnostní prvky zajišťující správu a ověření identity uživatelů, administrátorů a aplikací.

§20 Řízeni přístupových oprávněni

- Bezpečnostní prvky zajišťující centralizovaný nástroj pro řízení přístupových oprávnění k jednotlivým aktivům IKS (pro čtení dat, zápis dat a změnu oprávnění, atd.).

Možná řešení dle vyhlášky 82 ZoKB

§ 21 Ochrana před škodlivým kódem

- Bezpečnostní prvky zajišťující automatickou ochranu před škodlivým kódem u koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných nosičů, komunikační sítě a prvků komunikační sítě a obdobných zařízení

Možná řešení dle vyhlášky 82 ZoKB

§22 Zaznamenávání událostí IKS, jeho uživatelů a administrátorů, §23 Detekce KB událostí, §24 Sběr a vyhodnocování KB událostí

- Bezpečnostní prvky zajišťující zaznamenávání, sběr, detekci, analýzu a vyhodnocování bezpečnostních událostí IKS, jeho uživatelů a administrátorů

Možná řešení dle vyhlášky 82 ZoKB

§25 Aplikační bezpečnost

- Bezpečnostní prvky zajišťující trvalou ochranu aplikací, informací a transakcí před neoprávněnou činností a před popřením provedených činností.

§26 Kryptografické prostředky

- Kryptografické bezpečnostní prvky (včetně systému jejich správy) zajišťující ochranu aktiv IKS

Možná řešení dle vyhlášky 82 ZoKB

§27 Zajišťování úrovně dostupnosti informací

- Bezpečnostní a podpůrné prvky zajišťující dostupnost IKS a jeho odolnost vůči KB incidentům snižujícím jeho dostupnost.
- Technologické prostředky zajišťující dostupnost a redundanci důležitých technických aktiv IKS.

Nástroje kybernetické bezpečnosti §18 - §21

Nástroje kybernetické bezpečnosti (KB)		
Bezpečnostní opatření	**Bezpečnostní prvek**	**co zajišťuje**
§18 Bezpečnost komunikačních sítí	NGIPS (Datacentre Next generation IPS / firewall)	funkce firewallu, IPS sondy, sandboxing, URL filtrace, blokování podezřelého provozu atd.
§18 Bezpečnost komunikačních sítí	Radius server + 802.1X	systém pro řízení přístupu a autentizaci zařízení a uživatelů v LAN, WiFi, VPN prostřednictvím protokolu 802.1X
§18 Bezpečnost komunikačních sítí	Síťové prvky	segmentace sítě (fyzická, logická)
§18 Bezpečnost komunikačních sítí §25 Aplikační bezpečnost	WAF (webový aplikační firewall)	ochrana webových aplikací proti útokům, podezřelým aktivitám, zneužití relací uživatelů inspekcí webové komunikace a HTTP manipulací
§19 Správa a ověřování identit	IDM (Identity Management)	jednotná správa a ověřování elektronických identit uživatelů všech IS
§19 Správa a ověřování identit	PIM (Privileged Identity Management)	centrální správa a řízení privilegovaných identit na základě privilegovaných rolí (práv a oprávnění)
§20 Řízeni přístupových oprávněni	AM (Access Management)	jednotná správa a řízení (vytváření, přiřazování, odebírání, rušení) rolí, přístupových práv a oprávnění uživatelů všech IS
§20 Řízeni přístupových oprávněni	PAM (Privileged Access Management)	správa a řízení privilegovaných účtů a přístupů privilegovaných uživatelů k technickým aktivům (IS, serverům, aktivním prvkům)
§20 Řízeni přístupových oprávněni §21 Ochrana před škodlivým kódem	Mobile Device Management „MDM“ Antivirové prostředky	centrální správa a řízení přístupů k mobilním zařízením s antimalwarovým systémem antivirová ochrana koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných nosičů, komunikační sítě atd.

Nástroje kybernetické bezpečnosti §22 - §24

Nástroje kybernetické bezpečnosti (KB)		
Bezpečnostní opatření	**Bezpečnostní prvek**	**co zajišťuje**
§22 Zaznamenávání událostí IKS, jeho uživatelů a administrátorů §25 Aplikační bezpečnost	LM (Log Management) systém pro sběr, správu a řízení záznamů	zabezpečená centrální správa a řízení (sběr, agregace, dlouhodobé ukládání, archivace, prohlížení…) pořízených záznamů událostí a činností zajišťující trvalou ochranu aplikací, informací a transakcí před popřením provedených činností
§23 Detekce KB událostí §27 Zajišťování úrovně dostupnosti informací	Sonda pro záznam datových toků L2-L4, L7	zaznamenávání datového provozu pomocí NetFlow, sFlow nebo IPFIX
§23 Detekce KB událostí §27 Zajišťování úrovně dostupnosti informací	Kolektor	sběr, agregace a analýza zaznamenaných datových toků
§23 Detekce KB událostí §27 Zajišťování úrovně dostupnosti informací	NBAD (Network Behavior Anomaly Detection)	detekce bezpečnostních událostí na základě zjištěných anomálií a analýzou chování sítě
§24 Sběr a vyhodnocování KB událostí	SIEM (Security Information and Event Management)	sběr a agregace všech záznamů událostí a činností technických aktiv s následnou detekcí anomálií, podezřelých aktivit, bezpečnostních incidentů (útoků), hrozeb a trendů na základě nepřetržité analýzy dat dle stanovených požadavků a korelací.
§24 Sběr a vyhodnocování KB událostí	SOAR (Security orchestration, automation and response)	automatizace a optimalizace bezpečnostních procesů pro reagování na bezpečnostní události (z agregovaných bezpečnostních dat a výstrah) a pro standardizaci postupů detekce a nápravy hrozeb s integrací na SOC

Nástroje kybernetické bezpečnosti §25 - §27

Nástroje kybernetické bezpečnosti (KB)		
Bezpečnostní opatření	**Bezpečnostní prvek**	**co zajišťuje**
§25 Aplikační bezpečnost §27 Zajišťování úrovně dostupnosti informací	VMS (Vulnerability management System) Vulnerability SW nástroje-scannery	skenování, analyzování a náprava zjištěných zranitelností HW/SW řízení rizik na základě zjištěných zranitelností v případě, že se jedná o neopravené, nesprávně nakonfigurované a neznámé systémy
§25 Aplikační bezpečnost	Systém / SW nástroj pro penetrační testování	penetrační testování technických aktiv
§26 Kryptografické prostředky	kryptografické klíče, šifrovací algoritmy (symetrické klíče, asymetrické klíče, s využitím funkce hashování), systémy kryptografické ochrany hardwaru a softwaru, HSM (Hardware Security Module)	kryptografické klíče, kryptografické algoritmy, certifikáty včetně zajištění jejich ochrany systémem správy klíčů a certifikátů (pro generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů)
§27 Zajišťování úrovně dostupnosti informací	High availability řešení (ACTIVE – ACTIVE) Load balancing Záložní řešení	1. datová infrastruktura 2. serverová infrastruktura 3. síťová infrastruktura 4. virtualizační systémy 5. záložní infrastruktura a systémy

A co organizační bezpečnostní opatření ?

- Klasifikace a hodnocení aktiv
- Plán záloh a obnovy
- Plán zvládání rizik
- Pravidla pro vytváření účtů a řízení přístupu
- Systemizace pracovních míst
- Metodika pro detekci, vyhodnocování a hlášení KB incidentů
- Metodika pro zvládání KB incidentů
- Plán kontinuity činností
- Penetrační testy, testy zranitelností, atd.

Oblast eGovernmentu
Povinné dokumenty

Referenční dokumenty

- Příloha žádosti – Souhlasné stanovisko Hlavního architekta eGovernmentu
- Žádost o podporu
- Studie proveditelnosti

Oblast eGovernmentu
Hodnocení

Hodnocení projektů eGovernmentu (podmínky)

- projekt přináší inovace v podobě nových funkcionalit informačních systémů
- každý pořízený (nový nebo inovovaný) informační systém musí mít projektem zavedeny minimálně tři nové funkcionality
- projekt je v souladu s Prováděcím dokumentem programu Digitální Česko pro čerpání z IROP 2021–2027

Oblast eGovernmentu
Podmínky

Specifická kritéria projektů eGovernmentu = plnění 3 z níže uvedených možných funkcionalit:

- nová samoobslužná služba veřejné správy z katalogu služeb veřejné správy;
- přispívání do propojeného nebo datového fondu veřejné správy;
- interoperabilita na území státu pomocí referenčního rozhraní VS s přesahem i např. v rámci EU;
- logická centralizace a celoplošná dostupnost v rámci OVM a SPUU sdílejících ISVS nebo soukromoprávní systém pro využívání údajů;
- zvýšená spolehlivost, bezpečnost a průchodnost provozních informačních systémů, spravovaných jednotlivými OVM s využitím sdílení ICT platforem;
- lepší dostupnost služeb veřejné správy nebo interoperabilita na území státu s přesahem v rámci EU;
- využívání služeb národního bodu pro identifikaci a autentizaci;
- zavedení metod automatizace a robotizace ve veřejné správě;
- využívání služeb cloud computingu z katalogu služeb cloud computingu;
- budování ISVS s podporou samostatných a oddělených modulů (kontejnerů) komunikujících pomocí mikroslužeb se zabráněním vendor lock-in

Možné funkcionality ISVS

nové funkcionality ISVS	obecně parametry umožňující	možné řešení
nová samoobslužná služba veřejné správy z katalogu služeb veřejné správy	podporu samoobslužných procesů (poskytovaných služeb) veřejné správy, které využívají 1. občané nebo firmy bez nutnosti osobní návštěvy na úřadu a bez nutnosti zprostředkování služby veřejné správy úředníkem 2. úředníci veřejné správy bez nutnosti zprostředkování služby jiným zástupcem OVM	transakční portálová řešení pro: ▪ občany ▪ podnikatele ▪ úředníky ▪ soukromoprávní uživatele
přispívání do propojeného datového fondu veřejné správy	provedení integrace datového fondu s daty dostupnými prostřednictvím ISZR či eGSB a/nebo publikace údajů z datového fondu prostřednictvím eGSB pro příjemce v jiných agendách, aby bylo možné data sdílet a využívat i v jiných ISVS	IS využívající údaje z ISZR IS poskytující údaje do ISZR IS využívající údaje přes eGSB/ISSS IS poskytující údaje přes eGSB/ISSS
interoperabilita na území státu pomocí referenčního rozhraní veřejné správy s přesahem i např. v rámci EU	vytvoření nebo modernizace univerzálního rozhraní pro interoperabilitu a/nebo napojení na existující rozhraní pro interoperabilitu	integrační rozhraní na ISZR integrační rozhraní na eGSB/ISSS integrační rozhraní na FAIS integrace na portál gov.cz
logická centralizace a celoplošná dostupnost v rámci orgánů veřejné moci (OVM) a soukromoprávních uživatelů údajů (SPUU) sdílejících informační systém veřejné správy či soukromoprávní systém pro využívání údajů	poskytování celoplošně dostupných sdílených elektronických služeb pro organizace veřejné moci či soukromoprávní organizace	portálová řešení (portály úředníka) pro orgány veřejné moci (OVM) ▪ centrální (federující) portály ▪ agendové portály ▪ portály území ▪ weby publikující OpenData portálová řešení pro soukromoprávní uživatele údajů (SPUÚ)

Možné funkcionality ISVS

nové funkcionality ISVS	obecně parametry umožňující	možné řešení
zvýšená spolehlivost, bezpečnost a průchodnost provozních informačních systémů, spravovaných jednotlivými OVM s využitím sdílení ICT platforem	bezpečnou, důvěryhodnou a spolehlivou provozní podporu systémů podle definovaných provozních parametrů, s příslušnou provozní podporou včetně nastaveného provozního a bezpečnostního dohledu	▪ high availability řešení ▪ datová infrastruktura ▪ síťová infrastruktura ▪ serverová infrastruktura ▪ virtualizace ▪ záložní řešení
lepší dostupnost služeb veřejné správy nebo interoperabilita na území státu s přesahem v rámci EU	dostupné standardizované služby, napojené na existující rozhraní pro interoperabilitu, poskytující zabezpečení autentizace klientů od anonymních po nejvyšší záruky bezpečnosti	systémy umožňující: ▪ vzdálený bezpečný přístup v EU ▪ vícefaktorovou autentizaci ▪ autentizaci přes NIA ▪ autentizaci přes JIP/KAAS ▪ integraci na interní systémy ▪ integraci na externí systémy ▪ integraci na centrální systémy
využívání služeb národního bodu pro identifikaci a autentizaci	identifikaci a autentizaci osob pro zprostředkování samoobslužné služby veřejné správy prostřednictvím kvalifikovaných správců (poskytovatelů – providerů identit)	rozhraní pro integraci na národní bod pro identifikaci a autentizaci prostřednictvím Národní identitní autority (NIA)
zavedení metod automatizace a robotizace ve veřejné správě	zavedení automatizace a robotizace do vnitřních procesů a samoobslužných procesů (služeb) s doloženým přínosem pro zvýšení efektivity těchto procesů	nástroje pro digitalizaci dat ▪ skenování (digitalizaci) dokumentů ▪ optimalizaci obrazu a kategorizaci dokumentů ▪ přenesení metadat do předem definované struktury nástroje na automatizaci procesů ▪ integrační rozhraní, systémy ▪ identity access management ▪ datový sklad a nástroje BI nástroje pro robotickou automatizaci procesů (RPA) založenou na autonomní práci softwarových robotů

Robotická automatizace procesů (RPA) softwarová robotika

RPA umí ZPRACOVÁVAT digitální data v různých formátech, KOMUNIKOVAT se systémy a aplikacemi a NÁSLEDOVAT jasná procesní pravidla, využívá automatizační technologie k napodobování back-office úkolů lidských pracovníků, jako je

- extrahování dat
- vyplňování formulářů
- přesouvání souborů a složek
- otevírání e-mailu a příloh
- přihlašování do webových a podnikových aplikací
- kopírování a vkládání
- čtení a zápis do/z databází, systémů a aplikací
- získávání dat z webu
- připojení se k jiným systémům prostřednictvím API
- provádění výpočtů a validací
- extrahování strukturovaných dat z dokumentů
- shromažďování statistik ze sociálních médií
- rozhodování se podle pravidel typu „jestliže/pak“

Robotická automatizace procesů (RPA) softwarová robotika

RPA kombinuje rozhraní API a interakce uživatelského rozhraní (UI) pro integraci a provádění opakujících se úkolů mezi podnikovými a kancelářskými aplikacemi. Nasazením skriptů, které nahrazují (napodobují) lidské procesy, nástroje RPA dokončují autonomní provádění různých činností a transakcí napříč nesouvisejícími softwarovými systémy.

Uplatnění automatických úkonů v rámci agend měst:

- Automatizace Odesílání upozornění
- Majetková správa
- Založení karty poplatníka (Narození, Přistěhování)
- Hlavní uzávěrky kódu poplatků
- Generování opravných položek
- Identifikace příjmů na účtech města
- Agenda komunální odpad
- Agenda poplatků za psa
- Přerozdělování datových zpráv
- Automatické přesouvání databázových dat
- Živnostenský úřad (Kontrola úhrady správních poplatků, Úhrady sankcí/pokut)

Děkuji za pozornost

barbora.stranska@gmail.com

+420602308384