

SEZNAM PLÁNOVANÝCH ZÁMĚRŮ PRO IROP 2021-2027 V RÁMCI AKTUALIZACE PROVÁDĚČÍHO DOKUMENTU (DUBEN 2024)

Název záměru	Popis	Předběžná doba realizace	Vazba na hlavní cíl IK ČR	Geoční úřad	Výdaje celkem [mil. Kč] (není předmětem hlasování)
PSIVÚ - Vývoj nejhodnějšího softwarového řešení platformy pro sdílení a integraci veřejných údajů (PSIVÚ)	<p>Cílem je vybudování platformy pro sdílení a integraci veřejných údajů (dále PSIVÚ) jako informačního systému veřejné správy, který je nedílnou součástí referenčního rozhraní veřejné správy a jehož prostřednictvím bude zajišťováno sdílení takových dat a služeb mezi informačními systémy veřejné správy, jejichž charakter neumožňuje sdílení pomocí současných možností informačního systému sdílené služby dle zákona č. 111/2009 Sb. Platforma bude vybudována tak, aby byla součástí globální architektury veřejného datového fondu a disponovala specifickými funkcionalitami:</p> <p>a) zajištění jednotlivým OVM a SPUÚ přístup ke garantovaným otevřeným datům ve VDF; b) dávkový přístup k obsahu jednoho nebo více údajů bez vazby na konkrétní subjekt práva, a to ke kompletnímu obsahu nebo k obsahu vázanému na jednu datovou položku (např. sdílení a výměna datových/informačních kontejnerů); c) sdílení prostorových informací a služeb, ale i neprostorových údajů; d) multikriteriální vyhledávání dat napříč jednotlivými zdroji dat; e) napojení na rozhraní EU dataspací; f) umožnění zpoplatnění sdílených dat;</p> <p>Cílem vybudování platformy pro sdílení a integraci veřejných údajů je vytvořit prostředí, ve kterém bude možno orgánům veřejné moci na základě dostupných datových sad prostředkovat tato data prostřednictvím definovaných služeb pro:</p> <p>-řzhodování v agendách veřejné správy (na základě poptávky jednotlivých agend rozbořením právních předpisů) s ohledem na kompetence vymezené legislativou (v kontextu registru práv a povinností),</p> <p>-řpublikační místa pro veřejnost (národní geoportál, Czech POINT, datové schránky, webové služby).</p> <p>Platforma pro sdílení a integraci veřejných údajů vychází z konceptu sdílených služeb, bude součástí infrastruktury eGovernmentu České republiky a bude respektovat požadavky stanovené zákonem o kybernetické bezpečnosti.</p>	26.09.2022 - 30.09.2025	Cíl č. 5 - Efektivní a centrálně koordinované ICT veřejné správy	DIA (Digitální informační agentura)	150
Psychiatrická nemocnice v Kroměříži - kyberbezpečnost	<p>Projekt má za cíl vybudovat zabezpečené prostředí pro chod informačních systémů nemocnice s důrazem na ochranu integrity a důvěrnosti dat. Cílem je zavedení technických opatření, která budou zabezpečovat kybernetickou bezpečnost základních a podpůrných informačních systémů podle požadavků ZKB a NIS2. Navazuje na cíle strategie Zdraví 2030 a její prioritní oblast 3.5 Digitalizace zdravotnictví pořízením robustní IT infrastruktury s vysokou úrovní kybernetické bezpečnosti.</p> <p>Projekt vybuduje bezpečné prostředí pro běh informačního systému nemocnice v prostředí se segmentovanou sítí s chráněným perimetrem. Nové aktivní prvky zajistí řízení komunikace v rámci komunikační sítě a jejího perimetru. Pomocí kryptografie zajistí důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií.</p> <p>Klíčovým faktorem bezpečnosti dat je ověření lékáře, či jiného zdravotnického pracovníka, a správa jeho identity, aby se k citlivým údajům o pacientovi dostal jen oprávněný personál. S tím souvisí i řízení přístupů a správa identit s nimi propojených v nemocnici tak, aby tyto informace nebo služby byly přístupné pouze povolaným osobám.</p> <p>Uživatelé budou moci přistupovat do systémů po dvoufaktorovém ověřování a jejich identita bude centrálně spravována. Současně však také bude sledována činnost privilegovaných účtů, kdy bude zavedena jejich centrální správa se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům včetně zajištění transparentního přihlášení. Rizikovost akcí jak u privilegovaných účtů, tak u běžných uživatelů, bude hodnocena a případné rizikové akce nebudou dovoleny.</p> <p>Děni ve vnitřní síti bude pečlivě monitorováno a kybernetické hrozby budou detekovány. Detekční systém zaznamenává události v rámci infrastruktury a dává je k dispozici odpovědným osobám (rolím) pro vyhodnocení dopadů činnosti a s upozorněními na události, či hrozby. Proto bude pořízen pokročilý nástroj pro analýzu síťového provozu, sledování výkonu, detekci hrozeb a rizik s hloubkou viditelností do sítě pro ochranu vnitřní sítě. Systém také zajistí blokování nežádoucí komunikace, ochranu všech aktiv v síti od koncových stanic přes mobilní zařízení až po servery. V rámci projektu bude realizováno:</p> <p>-řzavedení systému řízení bezpečnosti informací a báze znalostí v oblasti kybernetické bezpečnosti včetně souvisejících procesů a dokumentace</p> <p>-řpořízení de-duplikační jednotky pro zvýšení dostupnosti a celkové retence záloh</p> <p>-řpořízení zálohovací páskové knihovny (předpoklad LTO09, WORM)</p> <p>-řpořízení fyzického zálohovací serveru</p> <p>-řpořízení zavedení dynamické segmentace (NAC, 802.11), pro bezpečný přístup k podnikové síti, zajistí bezpečný a oddělený přístup zaměstnanců a pacientů</p> <p>-řpořízení a implementace nástroje pro řízení přístupů a identit, správa přístupů na kritické systémy infrastruktury (PIM/PAM)</p> <p>-řpořízení a implementace NGFW (Next Generation Firewall), včetně WAF (Web Application Firewall)</p> <p>-řpořízení a implementace systému RSD (bezpečný vzdálený přístup k aplikacím), zabezpečení přístupu ke koncovým zařízením pomocí dvou-faktorové autentizace uživatelů</p> <p>-řpořízení a nasazení antivirového systému včetně EDR (Endpoint Detection and Response)</p> <p>-řpořízení a implementace NDR (Network Detection & Response), SW nástroj pro síťovou detekci bezpečnostních hrozeb, vizualizace síťové komunikace, analýza síťového provozu, detekce škodlivých aktivit</p> <p>-řpořízení a vybudování DR prostředí, HW+SW infrastruktura nezbytná pro běh pořízených bezpečnostních technologií a pro zajištění business continuity (servery, storage, síťové prvky, licence)</p>	01.06.2023 - 31.05.2026	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	37,37
Zvýšení kybernetické bezpečnosti Městské nemocnice Čáslav	<p>-řzavedení systému řízení bezpečnosti informací a báze znalostí v oblasti kybernetické bezpečnosti včetně souvisejících procesů a dokumentace</p> <p>-řpořízení de-duplikační jednotky pro zvýšení dostupnosti a celkové retence záloh</p> <p>-řpořízení zálohovací páskové knihovny (předpoklad LTO09, WORM)</p> <p>-řpořízení fyzického zálohovací serveru</p> <p>-řpořízení zavedení dynamické segmentace (NAC, 802.11), pro bezpečný přístup k podnikové síti, zajistí bezpečný a oddělený přístup zaměstnanců a pacientů</p> <p>-řpořízení a implementace nástroje pro řízení přístupů a identit, správa přístupů na kritické systémy infrastruktury (PIM/PAM)</p> <p>-řpořízení a implementace NGFW (Next Generation Firewall), včetně WAF (Web Application Firewall)</p> <p>-řpořízení a implementace systému RSD (bezpečný vzdálený přístup k aplikacím), zabezpečení přístupu ke koncovým zařízením pomocí dvou-faktorové autentizace uživatelů</p> <p>-řpořízení a nasazení antivirového systému včetně EDR (Endpoint Detection and Response)</p> <p>-řpořízení a implementace NDR (Network Detection & Response), SW nástroj pro síťovou detekci bezpečnostních hrozeb, vizualizace síťové komunikace, analýza síťového provozu, detekce škodlivých aktivit</p> <p>-řpořízení a vybudování DR prostředí, HW+SW infrastruktura nezbytná pro běh pořízených bezpečnostních technologií a pro zajištění business continuity (servery, storage, síťové prvky, licence)</p>	01.06.2024 - 31.05.2026	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	24,6
Zvýšení kybernetické bezpečnosti KHS Plzeň	<p>KHS si klade za cíl zvýšit kybernetickou bezpečnost IT systémů, které používá ke své činnosti. KHS při své běžné činnosti zpracovává citlivá data obyvatel ČR a dále zaměstnanců KHS. Z uvedených důvodů by KHS v případě možné alokace finančních prostředků zakoupila a vyměnila za stávající switche za nové.</p> <p>Primárním cílem je inovace části počítačové sítě KHS Plzeňského kraje formou náhrady zastaralých a výrobcem již nepodporovaných přepínačů HP 1910-48G, 1910-24G a 1810-8G a Mikrotik tak, aby byla zajištěna požadovaná dostupnost souvisejících služeb. Zastaralá a výrobcem nepodporovaná zařízení je nutno průběžně nahrazovat novými jednak proto, aby bylo možno zachovávat požadovanou dostupnost služeb počítačové sítě KHS Plzeňského kraje formou záruky výměny porouchaného zařízení novým v požadované době, a jednak i z bezpečnostních a provozních důvodů, neboť výrobcem nepodporovaná zařízení již nezaručují bezchybnou funkčnost, zejména protože neumožňují nezbytnou průběžnou aktualizaci svého programového vybavení odstraňujícího nalezené chyby. Potenciální alternativní možnost navýšení vlastních skladových zásob pro nahrazování porouchaných zařízení s uplynulou záruční lhůtou nepřipadá v tomto případě v úvahu, protože se jedná vesměs o výrobce již nepodporovaná zařízení, pro která tedy neexistuje žádná možnost oprav možných chyb programového vybavení, tedy ani zajištění jejich správné funkčnosti.</p> <p>Předpoklad ceny cca 140.000,- Kč. Můžeme doložit podrobnosti.</p> <p>KHS by dále v rámci zvýšení kybernetické bezpečnosti chtěla zvýšit zabezpečení e-mailové komunikace. Nákup a nasazení Fortine FortiMail 200F. Zvýšení bezpečnosti e-mailové komunikace dle doporučení NÚKIBu. Jedná se o zařízení, které chrání emailový server proti spamu, malware a dalším e-mailovým hrozbám. S FortiMail lze zabránit tomu, aby byl náš systém i lidské zdroje zahlceni nevyžádanou poštou. V příchozím směru FortiMail efektivně blokuje spam a malware. Jeho filtr příchozí pošty zlikviduje spam a malware dříve, než dojde k odeslání zprávy, na úrovni TCP spojení. V odchozím směru kontroluje jednotlivé zprávy tak, aby nedošlo k zařazení našeho systému do blacklistu. FortiMail umožňuje dynamicky i staticky kontrolovat jednotlivé uživatele, vlivem čehož získáme kompletní kontrolu nad bezpečnostními politikami a uživateli. FortiMail poskytuje Identity – Based Encryption (IBE), kterou lze použít pro bezpečné doručení zpráv (metoda push nebo pull).</p> <p>Předpoklad ceny cca 110.000,- Kč. Můžeme doložit podrobnosti.</p>	01.08.2023 - 31.12.2023	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	1,25
Navýšení kybernetické bezpečnosti - Nemocnice Letovice	<p>Nemocnice Letovice poskytuje občanům preventivní, léčebnou, diagnostickou, léčebně rehabilitační, ošetrovatelskou a paliativní péči. Aby bylo možné provozovat výše zmíněné činnosti, je potřeba zajistit konzistentní technologický systém s vysokou dostupností, zajištěním integrity a důvěrnosti. V příloze je k dispozici dokument "Studie proveditelnosti", která řeší celkové neuspokojivou situaci v oblasti ochrany IS/KS a síť Nemocnice Letovice, příspěvkové organizace z pohledu standardů zákona o kybernetické bezpečnosti.</p>	01.07.2023 - 30.06.2025	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	15,06
Kybernetická bezpečnost IS Nemocnice Kyjov, příspěvková organizace	<p>Cílem tohoto projektu je zajistit soulad Nemocnice Kyjov jakožto provozovatele informačních a komunikačních systémů, jenž zpracovává, zprostředkuje a ukládá citlivé údaje, s požadavky Zákona o kybernetické bezpečnosti a s prováděcí vyhláškou. Technická opatření navrhovaná tímto projektem směřují právě k zajištění souladu s požadavky zákona, čímž přispějí k předcházení hrozeb kybernetických a bezpečnostních incidentů. Výsledkem projektu tedy bude posílení ochrany informačních a komunikačních systémů žadatele před kybernetickými útoky. V rámci projektu budou technická opatření zabezpečena v rámci 6 aktivit: Realizace nástroje pro řízení přístupu na síti, Implementace nástroje pro risk asset management, Skenner zranitelností a hardeningové politiky, Nástroj pro správu privilegovaných účtů, Nástroj pro sběr a korelaci událostí a logů – log management, Zajištění fyzické bezpečnosti datového centra. Podporovanou aktivitou této výzvy je kybernetická bezpečnost. Cíle projektu tuto aktivitu naplňují.</p>	01.04.2022 - 30.06.2025	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	18,46
Centrála NÚKIB pro zajištění kybernetické bezpečnosti ČR - Černá Pole	<p>Cíl projektu: Zajistit a zvýšit úroveň kybernetické bezpečnosti kritické informační infrastruktury NÚKIB v nově vybudované centrální lokalitě NÚKIB včetně vybudování a zabezpečení nového multifunkčního kybernetického polygonu NÚKIB.</p> <p>Kybernetickou bezpečnost KII NÚKIB je v plánu zajistit skrze nové nebo modernizované prvky kybernetické bezpečnosti zejména v oblasti fyzické bezpečnosti, bezpečnosti komunikačních sítí, správy a ověřování identit, řízení přístupových oprávnění, ochrany před škodlivým kódem, sběru a vyhodnocování kybernetických bezpečnostních událostí, kryptografických prostředků a zajišťování úrovně dostupnosti informací. Cíle bude dosaženo v rámci aktuálně připravované stavby nové centrální administrativní budovy NÚKIB v Brně "Černá Pole", která se stane novou hlavní lokalitou NÚKIB a tedy i centrálním místem zajištění kybernetické bezpečnosti v ČR. Potřebná úroveň doplnění a rozšíření zabezpečení KII v kontextu nové budovy a budoucích stavů zaměstnanců i infrastruktury efektivně navazuje na již realizované projekty a nákupy do dosavadních lokalit a infrastruktury NÚKIB. V případě dramatického prodloužení výstavby centrální budovy existuje náhradní varianta s omezeným rozsahem.</p>	01.01.2021 - 31.12.2028	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Národní úřad pro kybernetickou a informační bezpečnost	439,72