projekt_2722_Projektovy_zamer_ramcovy

PROJEKTOVÝ ZÁMER

Vzor pre manažérsky výstup I-02

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	Technická univerzita vo Zvolene
Názov projektu	Zvýšenie úrovne kybernetickej bezpečnosti na Technickej univerzite vo Zvolene
Zodpovedná osoba za projekt	Ing. Tibor Weis (projektový manažér)
Realizátor projektu	Technická univerzita vo Zvolene
Vlastník projektu	Technická univerzita vo Zvolene

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Ing. Tibor Weis	TU Zvolen	Riaditeľ CIT	21.6.2024	

1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.1	01.06.2024	*Pracovný návrh*	Ing. Tibor Weis
1.0	21.06.2024	*Zapracovanie súladu s vyhláškou č. 401/2023 Z. z.*	Ing. Tibor Weis

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s Vyhláškou 401/2023 Z.z. je Projektový zámer určený na rozpracovanie detailných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, pláne realizácie, alokovaní rozpočtu a ľudských zdrojov.

Dokument Projektový zámer v zmysle vyššie uvedenej vyhlášky a prílohy č. 8 výzvy PSK-MIRRI-614-2024-DV-EFRR (Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy) obsahuje manažérske zhrnutie, motiváciu a rozsah projektu, zainteresované strany, ciele projektu a merateľné ukazovatele, návrh organizačného zabezpečenia projektu, alternatívy, opis obmedzení, predpokladov, tolerancií, opis požadovaných výstupov, náhľad architektúry, opis rozpočtu, detailný popis nákladov a prínosov, postup a spôsob nacenenia projektu, harmonogram projektu a zoznamom rizík a závislostí.

V zmysle usmernenia MIRRI SR sa v projektovej dokumentácii (ani v ŽoNFP) nešpecifikujú detailne konkrétne riziká a dopady a nezverejňuje sa podrobná dokumentácia toho, kde sú najväčšie riziká IT systémov a uvádzajú sa iba oblasti identifikovaných rizík a dopadov. Rovnako sú v zmysle usmernenia MIRRI SR manažérske produkty napísané všeobecne.

2.1. Použité skratky a pojmy

Z hľadiska formálneho sú použité skratky a pojmy rámci celého dokumentu definované priebežne, štandardne pri prvom použití v zátvorke označením („ďalej len“).

2.2. Konvencie pre typy požiadaviek (príklady)

V rámci projektu budú definované tri základné typy požiadaviek:

Funkčné (používateľské) požiadavky majú nasledovnú konvenciu:

IDxx

ID – funkčná požiadavka xx – číslo požiadavky

Nefunkčné (kvalitatívne, výkonové - Non Functional Requirements - NFR) požiadavky majú nasledovnú konvenciu:

IDxx

ID – nefukčná požiadavka (NFR) xx – číslo požiadavky

Technické požiadavky majú nasledovnú konvenciu:

IDxx

ID – technická požiadavka xx – číslo požiadavky

3. DEFINOVANIE PROJEKTU

3.1. Manažérske zhrnutie

Technická univerzita vo Zvolene (ďalej len „TUZVO“) ako významná vzdelávacia a výskumná inštitúcia na Slovensku sa stretáva s rastúcimi požiadavkami na zabezpečenie kybernetickej bezpečnosti. V dnešnej digitálnej dobe je ochrana citlivých údajov, výskumných dát a osobných informácií študentov a zamestnancov kľúčová.

TUZVO zabezpečuje online služby pre viac ako 500 zamestnancov a približne 2000 študentov. Pri takomto počte potenciálnych používateľov je dôležité zabezpečiť zvýšenú úroveň ochrany pred internetovými hrozbami. Na zabezpečenie plynulého chodu univerzity, výučby a správy používateľov sa používa množstvo informačných systémov. Dôležitosť kybernetickej bezpečnosti je z tohto pohľadu vysoká, pretože dopad potenciálneho kybernetického incidentu na univerzitu by zasiahlo do každodenného chodu a ovplyvnilo by veľké množstvo používateľov.

Hlavným cieľom projektu “Zvýšenie úrovne kybernetickej bezpečnosti na Technickej univerzite vo Zvolene” je rozvoj a zabezpečenie informačnej bezpečnosti v prostredí TUZVO a zabezpečiť súlad so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „zákon o KB“). TUZVO síce zatiaľ nespadá pod tento zákon, ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce.

Hlavným cieľom projektu je zvýšenie miery ochrany informačných systémov univerzity voči potenciálnym kybernetickým incidentom. Uvedené bude dosiahnuté prostredníctvom realizácie hlavnej aktivity projektu, ktorou je :

- **Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti**

Podaktivity projektu boli zvolené ako najkritickejšie oblasti kybernetickej bezpečnosti. Povinnými podaktivitami projektu sú:

- Vypracovanie a prijatie samostatného dokumentu Stratégia kybernetickej bezpečnosti
- Vytvorenie bezpečnostných politík kybernetickej bezpečnosti

Keďže žiadateľ tejto výzvy aktuálne nemá vypracované povinné podaktivity projektu, budú realizované v rámci projektu. Medzi ostatné podaktivity projektu patria:

TUZVO plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním nasledovných krokov:

- vytvorením katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach,
- vytvorením, resp. aktualizovaním kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.,
- implementáciou technických riešení podporujúcich riadenie bezpečnosti pri prevádzke,
- implementáciou systému na nepretržitú kontrolu dátových tokov v interných sieťach univerzity,
- implementáciou automatického nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou,
- implementáciou centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov,
- implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov,
- implementáciou nástroja na centrálne riadenie ochrany pred škodlivým kódom,
- implementáciou nástroja na detekciu, nástroja na zber a nepretržité vyhodnocovanie a evidenciu kybernetických bezpečnostných udalostí,
- zavedením nástroja určeného na notifikovanie o existujúcich zraniteľnostiach programových prostriedkov a ich častí,
- zvýšením bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít,
- vypracovaním plánov kontinuity a ich otestovaním,
- implementáciou systémov na správu a inventarizáciu aktív,

Úspešná realizácia projektu umožní dosiahnuť významný pokrok v zabezpečení systémov, nastavení procesov a zvýšenie spoľahlivosti počítačovej siete na TUZVO. Vďaka nasadeniu systémov, ktoré zvýšia bezpečnosť siete, bude možné naplniť merateľné ukazovatele, ktorými sú:

- Počet nasadených nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov
- Zvýšenie kapacity pre zálohovanie informačných systémov TUZVO
- Zvýšenie počtu prostriedkov a ich výkonu a detegovanie internetových hrozieb a ochranu dát používateľov

V dokumente Národná koncepcia informatizácie verejnej správy Slovenskej republiky z roku 2021 zaradilo Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky medzi priority v informatizácii verejnej správy aj kybernetickú a informačnú bezpečnosť. Tá má okrem iného posilňovať ľudské kapacity, minimalizovať bezpečnostné incidenty a škody a zvyšovať úroveň ekosystému kybernetickej a informačnej bezpečnosti. S rovnakým zámerom je predkladaný aj tento projekt. Úspešná realizácia projektu prispeje významnou mierou k naplneniu zámerov tejto koncepcie.

Po implementácii projektu bude TUZVO pripravená efektívnejšie riadiť informačnú a kybernetickú bezpečnosť (ďalej iba „IB“ a „KB“) a čeliť interným a externým hrozbám v oblasti IB a KB. TUZVO v súčasnosti nedisponuje dostatočnými finančnými, technologickými a personálnymi zdrojmi, aby mohla plnohodnotne vykonávať všetky potrebné aktivity v rozsahu požadovanom zákonom o KB. Hlavnými beneficientom projektu je TUZVO a jej jednotliví zamestnanci, resp. užívatelia informačných systémov. Nepriamym beneficientom sú študenti a osoby, resp. subjekty komunikujúce s UIS. V dôsledku zavedených opatrení, ktoré zvýšia mieru ochrany informačných systémov bude minimalizovaný výpadok, resp. negatívny dopad bezpečnostných incidentov na riadnych chod univerzity.

Ciele projektu

Ciele projektu sú definované v súlade s Národnou koncepciou informatizácie verejnej správy (ďalej len „NKIVS“):

- Zabezpečenie bezpečnosti prevádzky IS a sietí vrátane sieťovej a komunikačnej bezpečnosti
- Zaznamenávanie udalostí a monitorovanie a riešenie KIB incidentov
- Zabezpečenie kontinuity prevádzky

Dané ciele budú dosiahnuté realizáciou hlavnej aktivity projektu - Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti.

Cieľová skupina

Cieľovou skupinou sú zamestnanci TUZVO, študenti TUZVO, dodávatelia TUZVO a ostatné právnické osoby využívajúce systémy TUZVO.

Realizáciou aktivít projektu dosiahne TUZVO naplnenie hlavného cieľa, ktorým je zvýšenie informačnej a kybernetickej bezpečnosti a zabezpečenia ochrany údajov a elektronických dát, ktoré sú využívané TUZVO, zamestnancami ako aj študentmi.

Projekt je v súlade s intervenčnou stratégiou Programu Slovensko 2021-2027 v nasledovných oblastiach:

- súlad projektu so špecifickým cieľom: RSO1.2 (opatrenie 1.2.1)
- súlad s očakávanými výsledkami definovanými v Partnerskej dohode pre špecifický cieľ RSO 1.26 3) súlad s definovanými typmi oprávnených aktivít v rámci výzvy.

Realizáciou projektu budú naplnené nasledovné merateľné ukazovatele:

PO095 / PSKPSOI12 – cieľová hodnota 1

PR017 / PSKPRCR11 – cieľová hodnota 2400

Miesto realizácie: Technická univerzita vo Zvolene

Predpokladaný rozpočet projektu: **(oprávnených výdavkov) je 488 284,40 EUR s DPH.**

Technická univerzita vo Zvolene (ďalej „TUZVO“) momentálne nespadá pod Zákon o kybernetickej bezpečnosti (ďalej len ZoKB), ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce. TUZVO si nechala vypracovať nezávislé posúdenie kybernetickej bezpečnosti univerzity na základe požiadaviek ZoKB, z ktorého vyplynuli nesúlady s požiadavkami zákona. TUZVO si samozrejme uvedomuje potrebu zvyšovania kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám.

TUZVO si uvedomuje, že v zmysle požiadaviek zákona o kybernetickej bezpečnosti a zavedených opatrení v zmysle vyhlášky 362/2018 Z.z. (ďalej len ZoKB), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška 362/2018 Z.z.) nespĺňa niektoré požiadavky. Ide primárne o chýbajúcu, resp. neaktuálnu dokumentáciu a o niektoré technologické požiadavky, ktorých zaobstaranie je finančne náročné.

V prípade, že by mala TUZVO investovať do dobudovania kybernetickej bezpečnosti vlastné finančné prostriedky, je prakticky nereálne zrealizovať všetky povinnosti podľa zákona o kybernetickej bezpečnosti a zákona o informačných systémoch verejnej správy, nakoľko ide o pomerne vysoké náklady v krátkom časovom období.

S ohľadom na to, že univerzity majú limitované finančné zdroje na boj s kyberútokmi, a súčasne je ich povinnosťou dodržiavať ustanovenia zákona o ISVS a s vysokou pravdepodobnosťou bude musieť spĺňať aj požiadavky ZoKB o kybernetickej bezpečnosti, vyhlásilo MIRRI SR Výzvu, ktorá má umožniť aj inštitúciám ako TUZVO získať prostriedky na ochranu informačných systémov a dosiahnutie kybernetickej bezpečnosti na najvyššej úrovni pri minimálnych nákladoch.

Projekt je vypracovaný v súlade s nasledovným typom aktivity: Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy s definovanou hlavnou aktivitou: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti.

Sumarizácia hlavných parametrov hodnotenia predkladaného projektu:

P. č.	**Názov hodnotiaceho kritéria**	**Parametre v projekte**	**Zdroj**
1.	Miera rizík ohrozujúcich úspešnú realizáciu projektu	V rámci projektu bolo identifikovaných menej ako 10 % rizík z celkového počtu identifikovaných rizík v ŽoNFP s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu.	Príloha 1 zoznam rizík
2.	Administratívne, odborné a prevádzkové kapacity žiadateľa	Žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) dostatočné odborné kapacity s náležitou odbornou spôsobilosťou a know-how na riadenie a implementáciu projektu v danej oblasti. Popis zabezpečenia prevádzky riešenia je reálny, t. j. žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) personálne kapacity pre zabezpečenie prevádzky riešenia.	Informácie o projektovom tíme sú uvedené v PZ.
3.	Miera oprávnenosti výdavkov projektu	Všetky oprávnené aktivity vychádzajú z bodu 2 Výzvy a prílohy č. 8 Výzvy, ktorá definuje oprávnené podaktivity	**V rámci projektu budú realizované nasledovné oprávnené podaktivity:** · Organizácia kybernetickej a informačnej bezpečnosti · Riadenie rizík · Personálna bezpečnosť · Riadenie prístupov · Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami · Bezpečnosť pri prevádzke informačných systémov a sietí · Hodnotenie zraniteľností a bezpečnostné aktualizácie · Ochrana proti škodlivému kódu · Sieťová a komunikačná bezpečnosť · Zaznamenávanie udalostí a monitorovanie · Fyzická bezpečnosť a bezpečnosť prostredia · Kryptografické opatrenia · Kontinuita prevádzky · Audit a kontrolné činnosti
4.	Dôležitosť kybernetickej bezpečnosti u žiadateľa a potencionálny dopad kybernetických incidentov	V zmysle kapitoly 3.2.5 PODPORA V OBLASTI KIB NA REGIONÁLNEJ ÚROVNI uvedenej v prílohe 2 Výzvy boli Identifikované jednotlivé kategórie.	§ 24 ods. 2 písm. a) – kategória: I § 24 ods. 2 písm. b) a c) – kategória: I § 24 ods. 2 písm. d) – kategória: III §24 ods. 2 písm. e) – kategória: I

3.2 Motivácia a rozsah projektu

Vzhľadom k zvyšujúcim sa potrebám zabezpečenia infraštruktúry si TUZVO dala vypracovať v roku 2023 Analýzu úrovne informačnej a kybernetickej bezpečnosti. V dokumente bolo popísané nezávislé externé hodnotenie kybernetickej bezpečnosti. Ako šablóna pre túto analýzu sa zvolilo znenie Zákona o kybernetickej bezpečnosti 69/2018 Z.z. a znenie vykonávacej vyhlášky 362/2018 Z.z., ktorej novelizované znenie vošlo do platnosti 1.9.2023. Tento zákon a vyhláška pokrývajú celú škálu kybernetickej bezpečnosti a v blízkej dobe dôjde k transpozícii európskej smernice NIS2 do právneho systému Slovenskej Republiky.

Hlavnou motiváciou projektu je zvýšenie úrovne KIB, aby TUZVO bola lepšie pripravená čeliť interným a externým hrozbám v oblasti kybernetickej bezpečnosti.

Medzi hlavné ciele systému riadenia KIB patria:

- zabezpečenie správnej a bezpečnej prevádzky prostriedkov spracúvajúcich informácie,
- monitorovanie prostredia,
- evidencia a ošetrovanie podozrivých udalostí a bezpečnostných incidentov s dôrazom na prevenciu ich opakovaného výskytu.

Vyhlásená výzva „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy" súvisí najmä s naplnením povinností:

- definovanými v zákone č. 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB") a v zákone č. 95/2019 Z. z. Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS").
- opatreniami definovanými v § 20 zákona o KB.
- nutnosť zvýšenia úrovne a schopnosti zabezpečovať a riadiť informačnú a kybernetickú bezpečnosť vzhľadom na sústavne sa zvyšujúce hrozby a riziká,
- zabezpečenie realizácie spoločných blokov bezpečnostnej architektúry v súlade s NKIVS a strategickou prioritou informačnej a kybernetickej bezpečnosti,
- ako reakcia na aktuálny nedostatočný stav úrovne vyspelosti procesov riadenia KIB,
- ako reakcia na aktuálne zmeny v používaní IT, ako aj závažné útoky v oblasti kybernetickej bezpečnosti

Implementácia projektu

Implementácia projektu bude prebiehať v nasledovných krokoch:

Hlavná aktivita: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti:

- Prípravná fáza a Iniciačná fáza
- Realizačná fáza
    - Analýza a Dizajn
    - Nákup technických prostriedkov, programových prostriedkov a služieb
    - Implementácia a testovanie
    - Nasadenie opatrení
- Dokončovacia fáza
- Podpora prevádzky (SLA)

Podporné aktivity – nepriame výdavky

- Podporná aktivita – Projektový manažér interný/externý na riadenie hlavných aktivít projektu.
- Podporná aktivita – Publicita a informovanosť v zmysle manuálu

Súčasné bezpečnostné mechanizmy v oblasti monitoringu a hodnotenia zraniteľnosti implementované univerzitou tvoria základ, ktorý si vyžaduje ďalší rozvoj pre zaistenie primeranej ochrany spracúvaných informácií voči kybernetickým hrozbám a zároveň zabezpečenie súladu s povinnosťami vyplývajúcimi z ustanovení zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Okrem legislatívnych požiadaviek je nevyhnutné brať do úvahy aj aktuálny stav, ktorá je z časti spôsobený neschopnosťou včasnej detekcie možného kybernetického útoku z dôvodu absentujúcich bezpečnostných opatrení, chýbajúcich analytických nástrojov a nedostatku kvalitných zdrojov bezpečnostne relevantných záznamov.

V analýze informačnej a kybernetickej bezpečnosti bolo hodnotených viacero konkrétnych ukazovateľov úrovne zabezpečenia, ako sú:

- Stratégia kybernetickej bezpečnosti
- Personálne riadenie kybernetickej bezpečnosti
- Organizácia kybernetickej a informačnej bezpečnosti
- Riadenie rizík kybernetickej a informačnej bezpečnosti
- Personálna bezpečnosť
- Riadenie prístupov
- Bezpečnosť pri prevádzke informačných systémov
- Bezpečnosť pri prevádzke sietí
- Hodnotenie bezpečnostných zraniteľností
- Ochrana proti škodlivému kódu
- Sieťová a komunikačná bezpečnosť
- Monitoring sieťovej prevádzky
- Riešenie kybernetických incidentov

- Zabezpečenie kontinuity prevádzky

3.2.1 Hlavný popis problému

TUZVO momentálne nespadá pod Zákon o kybernetickej bezpečnosti (ďalej len ZoKB), ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce. TUZVO si nechala vypracovať nezávislé posúdenie kybernetickej bezpečnosti univerzity na základe požiadaviek ZoKB, z ktorého vyplynuli nesúlady s požiadavkami zákona. TUZVO si samozrejme uvedomuje potrebu zvyšovania kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám.

TUZVO si uvedomuje, že v zmysle požiadaviek zákona o kybernetickej bezpečnosti a zavedených opatrení v zmysle vyhlášky 362/2018 Z.z. (ďalej len ZoKB), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška 362/2018 Z.z.) nespĺňa niektoré požiadavky ktoré vyplynuli z analýzy. TUZVO postupne zavádza do praxe, avšak viaceré z nich predstavujú vysokú finančnú záťaž pre rozpočet univerzity a je prakticky nemožné zrealizovať ich z vlastných zdrojov. Práve tieto finančne náročné opatrenia, ktoré predstavujú najväčšie bezpečnostné riziká, sú predmetom predkladaného projektu.

Na rozdiel od súčasného stavu bude disponovať výrazne vyššími schopnosťami detekcie škodlivých aktivít, technologické vybavenie bude umožňovať lepšiu ochranu pred útokmi z externého a interného prostredia, ako aj ochranu dát.

TUZVO plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním nasledovných krokov:

- vytvorením katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach,
- vytvorením, resp. aktualizovaním kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.,
- implementáciou technických riešení podporujúcich riadenie bezpečnosti pri prevádzke,
- implementáciou systému na nepretržitú kontrolu dátových tokov v interných sieťach univerzity,
- implementáciou automatického nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou,
- implementáciou centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov,
- implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov,
- Implementáciou nástroja na centrálne riadenie ochrany pred škodlivým kódom
- implementáciou nástroja na detekciu, nástroja na zber a nepretržité vyhodnocovanie a evidenciu kybernetických bezpečnostných udalostí,
- zavedením nástroja určeného na notifikovanie o existujúcich zraniteľnostiach programových prostriedkov a ich častí,
- zvýšením bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít,
- vypracovaním plánov kontinuity a ich otestovaním,
- implementáciou systémov na správu a inventarizáciu aktív,

TUZVO má prijaté smernice ohľadom ochrany osobných údajov, ktoré čiastočne pokrývajú aj problematiku kybernetickej bezpečnosti. Taktiež je vypracovaný dokument „bezpečnostná politika“, ktorý čiastočne pokrýva požiadavky ZoKB. Tieto dokumenty je ale potrebné upraviť a aktualizovať tak, aby spĺňali požiadavky ZoKB. Z tohto dôvodu je jedným z cieľov projektu je vytvoriť a prijať všetky požadované náležitosti a dokumenty definované v prílohe č. 1 k vyhláške č. 362/2018 Z. z..

Nie je zavedený proces klasifikácie informácií je v súlade s požiadavkami vyhlášky č. 362/2018 Z. z. pre klasifikáciu informácií kategorizácia sietí a informačných systémov.

S ohľadom na vyššie uvedené bude teda predmetom projektu riešenie problematiky z nasledovných oprávnených oblastí podľa výzvy:

- Organizácia kybernetickej a informačnej bezpečnosti
- Riadenie rizík
- Personálna bezpečnosť
- Riadenie prístupov
- Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami
- Bezpečnosť pri prevádzke informačných systémov a sietí
- Hodnotenie zraniteľností a bezpečnostné aktualizácie
- Ochrana proti škodlivému kódu
- Sieťová a komunikačná bezpečnosť
- Zaznamenávanie udalostí a monitorovanie
- Fyzická bezpečnosť a bezpečnosť prostredia
- Kryptografické opatrenia
- Kontinuita prevádzky
- Audit a kontrolné činnosti

Hlavným problémom, ktorému TUZVO čelí je teda vyriešenie vyššie pomenovaných oblastí informačnej a kybernetickej bezpečnosti tak, aby bol dosiahnutý významný pokrok pri plnení súladu v oblasti príslušných predpisov KIB a súčasne aby boli technologické náležitosti KIB realizované tak, aby:

- chránili IT systémy, ktoré zabezpečujú prevádzku služieb univerzity pred kybernetickými útokmi
- plnili svoje úlohy počas implementácie i v čase udržateľnosti projektu,
- boli pripravené na ďalší rozvoj IT technológií a služieb poskytovaných univerzitou,
- a bolo možné ich flexibilne rozširovať bez ohrozenia prevádzkovaných i budúcich IT systémov.

Hlavné identifikované riziká a nedostatky

Najvyššia miera nesúladu s legislatívnymi požiadavkami kybernetickej bezpečnosti podľa ZoKB bola identifikovaná v nasledovných oblastiach:

- Potreba zavedenia formálneho riadenia KB primárne prípravou a úpravou potrebných bezpečnostných smerníc, politík a nariadení.
- Potreba implementácie HW a SW častí bezpečnosti siete a implementácie sieťovej bezpečnosti siete (dodávka firewallow, segmentácie sieťe a dohľadových systémov).
- Potreba riešenia problému absentujúceho systému pre zber, ukladanie a analýzu logov a vyhodnocovanie bezpečnostných udalostí (SIEM).
- Potreba zabezpečiť kontinuitu prevádzky, t.j. je potrebné zabezpečiť riadenie kontinuity kybernetickej bezpečnosti – túto problematiku je potrebné riešiť aj na úrovni BCM plánov a aj na úrovni technologickej.

Absencia základných smerníc - Stratégia kybernetickej bezpečnosti a bezpečnostné politiky

Vytvorenie bezpečnostnej dokumentácie je nevyhnutnou činnosťou, ktorá zabezpečí, aby táto dokumentácia reflektovala na skutkový stav a bola použiteľná pre reálne potreby žiadateľa. Absencia takéhoto systému zároveň spôsobuje vysokú mieru neznalosti:

- Zoznamu rozpoznaných zraniteľností, vrátane ich vlastníkov
- Zoznamu rozpoznaných hrozieb
- Zoznamu opatrení potrebných na potlačenie zraniteľností
- Identifikácie a ohodnotenia rizík na základe pravdepodobnosti hrozieb, uplatňovaných opatrení a dopadov na žiadateľa a pod.

Absencia havarijných plánov a plánov obnovy (BCM)

Absencia riadenia kontinuity činností (BCM) je problémom v podmienkach TUZVO, ktorý sa prejaví najmä v prípade krízových situácií, kedy je nevyhnutné zabezpečiť funkčnosť a dostupnosť extrémne dôležitých funkcií univerzity ta, aby bola schopná poskytovať svoje služby aj počas krízovej situácie, akou môže byť napríklad hackerský útok, požiar, živelná pohroma a pod. Práve absencia efektívne nastaveného BCM by spôsobila v prípade takejto mimoriadnej udalosti vysoké finančné a hospodárske škody.

Absencia manažéra kybernetickej bezpečnosti (MKB)

Manažér kybernetickej bezpečnosti (MKB) je v slovenských podmienkach nová riadiaca pracovná pozícia. Zodpovedá za niekoľko oblastí priamo alebo nepriamo súvisiacich s kybernetickou a informačnou bezpečnosťou, má mať možnosť komunikovať a predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu. Základné požiadavky, ktoré sa kladú na pozíciu manažéra kybernetickej bezpečnosti sú priamy prístup ku štatutárnemu orgánu a nezávislosť od prevádzky. MKB má mať možnosť komunikovať a predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu. Postavenie MKB musí byť nezávislé od útvaru zaisťujúceho prevádzku IT. Úlohou MKB je najmä zaistiť odolnosť organizácie voči kybernetickým bezpečnostným hrozbám, riadiť súvisiace riziká a riešiť bezpečnostné incidenty.

Absencia nástroja na riadenie a monitorovanie dostupných technologických kapacít dôležitých sieťových zariadení a služieb

V podmienkach TUZVO sa ako jeden z výrazných nedostatkov prejavuje absencia sofistikovaného nástroja na automatizované monitorovanie dostupných technologických kapacít dôležitých sieťových zariadení a služieb, ktorý by umožnil v dostatočnom časovom predstihu upozorniť žiadateľa na dosahovanie limitu normovanej kapacity zariadení (napr. voľný priestor na HDD, maximálnu kapacitu servera a pod.). Uvedené spôsobuje problémy pri prípadnom dopĺňaní potrebných kapacít, čo značne ovplyvňuje funkčnosť systémov žiadateľa.

Absencia bezpečnostného monitoringu v IKT prostredí

Sieťová infraštruktúra univerzity vyžaduje komplexné zabezpečenie voči neoprávnenému vstupu do internej siete. Existujúce zabezpečenie už nevyhovuje požiadavkám súčasnej doby. V rámci sieťovej infraštruktúry absentuje SIEM nástroj a SOC, ktoré by zabezpečili dozor voči kybernetickým bezpečnostným incidentom. Absencia takéhoto spôsobu ochrany kybernetického priestoru žiadateľa znemožňuje flexibilne reagovať na prípadné kybernetické incidenty a minimalizovať tak reakčnú dobu na incident a eliminovať škody z neho vyplývajúce.

Nedostatočná úroveň zálohovania

Hlavným prostriedkom pre fungovanie univerzity a jej služieb sú informačné technológie a elektronizácia, ktorá v súčasnosti tvorí základný kameň fungovania každodenných procesov. Všetky dáta sú tak ukladané v elektronickej podobe, problém však môže vzniknúť v prípade ak príde k zlyhaniu techniky a strate dát. Za účelom eliminácie tohto rizika je nevyhnutné vytvoriť efektívny spôsob zálohy dát, ktorý v súčasnej dobe nie je vybudovaný na dostatočnej úrovni a na zálohovanie dát sa využívajú staršie zariadenia s otáznou životnosťou.

Absencia centrálneho logovacieho systému

V organizácii absentuje spoločný systém na zaznamenávanie udalostí z centrálnych sieťových prvkov a serverov, služieb prístupných do externých sietí a kritických interných serverov a služieb. Všetky udalosti sú zaznamenávané len lokálne na jednotlivých systémoch.

Vyššie uvedené oblasti predstavujú najvýznamnejšie problémy TUZVO v oblasti informačnej a kybernetickej bezpečnosti. Ich eliminácia v kombinácii so systematickým riešením iných úloh v oblasti bezpečnosti IT systémov, ktoré žiadateľ kontinuálne vykonáva z vlastného rozpočtu, umožní dosiahnuť uspokojivú úroveň bezpečnosti informačných systémov univerzity a jeho kybernetickej bezpečnosti v súlade s Národnou koncepciou informatizácie verejnej správy Slovenskej republiky.

Informačné systémy v správe TUZVO

Univerzitný informačný systém (UIS)

Webový informačný systém pre podporu komplexného riadenia procesov univerzity, obsahuje nasledovné agendové moduly:

- *Študijný systém* – komplexné pokrytie pedagogického procesu od prijímacieho konania po záverečné štátne skúšky. Aplikácie riešia špecifické prístupy uchádzačov o štúdium, študentov, študijné referentky, pedagógov ako aj vedúcich pracovníkov a workflow schvaľovacích procesov, ktoré súvisia so štúdiom. Modul obsahuje elektronické prijímacie konanie, financovanie štúdia, e-learningové projekty, testovanie, prihlasovanie na skúšky, agendu záverečných prác, štátnych skúšok a množstvo ďalších podporných aplikácií.
- *Veda a výskum* – evidencia projektov, evidencia publikácií, bodové evaluácie pedagogických a tvorivých zamestnancov, tvorba životopisov
- *Zahraničné oddelenie* – evidencia zahraničných dohôd a inštitúcií, evidencia študijných pobytov zahraničných študentov na univerzite a evidencia výjazdov študentov TUZVO
- *eAgenda* –správa areálov, budov, miestností, rezervácia miestností, kontaktné centrum, správa elektronických prieskumov, správa elektronických hlasovaní, Centrálny bankový účet
- *Osobný manažment* – poštová schránka, dokumentový server. správa úloh, blogov a diskusné fóra
- *Portál verejných informácií* – portál pre publikovanie údajov z interných modulov UIS pre verejnosť (pracoviská používatelia, rozvrhy, predmety, študijné plány, záverečné práce, absolventi, ..)
- *Manažérska nadstavba* – portál vedúceho pre manažment pracoviska na všetkých úrovniach (vedúci pracoviska/katedry/ústavu, prodekani, dekani, rektor)
- *Technologický subsystém* – prístupový systém, management univerzitnej siete, správa účtov, prepojenie na Active Directory, synchronizácia hesla užívateľa z UIS do AD, dátové štruktúry pre generovanie LDAP, teda dáta pre autorizáciu a autentizáciu užívateľov pre prístup k službám.
- *Správa a prevádzka systému* –správa osôb a oprávnení, nastavenie hesiel, správa orgánov univerzity, správa číselníkov, zverejňovanie zásadných informácií. delegovanie zmeny identít, záznam operácií užívateľov,
- *Administratíva študentských domovov* – modul pre komplexnú správu ubytovaných študentov (podanie žiadosti o ubytovanie, sledovanie stavu vybavenia žiadosti, prihlasovanie sa na termín ubytovania/odubytovania, správa poplatkov za ubytovanie, ...)
- *Mobilná aplikácia* – zjednodušená verzia UIS pre mobilné zariadenia určená primárne pre študentov, umožňuje prijímanie push notifikácií generovaných hromadne v UIS

Prepojenia s externými systémami:

- Centrálny register študentov (**CRŠ**) – generovanie dávok pre CRŠ, vkladanie výstupov z CRŠ, validácia stavu v CRŠ a v UIS
- Centrálny register záverečných prác (**CRZP**) – rieši prenos súborov záverečných prác a metadát k prácam pre kontrolu originality záverečných prác
- Centrálny register zmlúv (**CRZ**) – automatický prenos zmlúv o ubytovaní na portál CRZ
- Centrum vedecko-technických informácií (**CVTI**) – generovanie výkazov z Prijímacieho konania
- Ekonomický systém **SOFIA** – prepojenie v oblasti posielania údajov o poplatkoch za prijímacie konanie, o školnom a štipendiách
- Registratúrna kniha **MEMPHIS** –
- Prepojenie UIS s cloudovou službou **Microsoft Office 365** – možnosť voľby poštového klienta pre spracovanie elektronickej pošty, predmetové tímy a akcie v MS Teams, možnosť prenosu rôznych typov udalostí vznikajúcich v UIS
- Knižničný systém **Academic Library** – import publikácií z knižničného informačného systému do UIS

Webové sídlo tuzvo.sk

Webová stránka zabezpečujúca prístup k informáciám o univerzite, obsahuje informácie napr. o možnostiach štúdia na TUZVO, o akreditovaných študijných programoch, harmonogramoch výučby a kontaktné údaje.

Ekonomický systém SOFIA

Ekonomický systém univerzity, prevádzkovaný v Datacentre MŠ VVaM SR, prístup do systému je možný iba s použitím VPN klienta.

Dochádzkový systém INFOS

Rieši komplexnú evidenciu dochádzky a prenos dát do Ekonomického systému SOFIA.

Prístupový systém Access

Zabezpečuje riadenie vstupov do objektov.

Registratúra RK Memphis

Evidencia všetkých vstupných, výstupných a interných dokumentov na TUZVO.

Stravovací systém Kredit

Komplexné riešenie stravovania zamestnancov a študentov (objednávanie, platby, výstupy pre Ekonomický systém SOFIA, tankovacie automaty pre dobíjanie kreditu a výdajné terminály, normovanie jedál).

3.2.2 Biznis procesy

Predmetom realizácie projektu bude zavedenie a IT podpora nasledovných business procesov:

- Riadenie prevádzky siete a informačného systému
- Zaznamenávanie, monitorovanie a riešenie incidentov kybernetickej bezpečnosti
- Zabezpečovanie kontinuity prevádzky

Okrem samotného zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS sa projekt bude dotýkať prakticky všetkých biznis procesov, ktoré sú vykonávané Technickou univerzitou vo Zvolene, a ktoré sú realizované prostredníctvom informačných systémov TUZVO za účelom poskytovania univerzitných služieb.

3.2.3 Oblasti zamerania projektu

Projekt sa primárne zaoberá oblasťou zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS. Ako bude uvedené ďalej, tento projekt má priamy dopad na všetky ISVS a technologické platformy, ktoré sú určené na poskytovanie služieb univerzity TUZVO, nakoľko výsledky projektu budú ochraňovať všetky IS pred potenciálnymi hrozbami kybernetickej a informačnej bezpečnosti.

Riešenie vyššie popísaných problémov bude dosiahnuté prostredníctvom súboru technických opatrení, ktoré vzájomnou kombináciou prispejú k vytvoreniu efektívneho systému ochrany informačnej infraštruktúry TUZVO. S ohľadom na uvedené sa bude realizácia projektu orientovať prioritne na nasledovné technické riešenia:

Vytvorenie a prijatie dokumentu Stratégia kybernetickej bezpečnosti

Stratégia kybernetickej bezpečnosti určuje ciele, ktoré je potrebné na základe výsledkov analýzy rizík kybernetickej bezpečnosti dosiahnuť, spolu s uvedením základných princípov na ich dosiahnutie a určením právomocí a zodpovedností za systémy manažérstva, riadenie rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie. Dokument Stratégia kybernetickej bezpečnosti, ktorý bude obsahovať:

- strategické ciele v oblasti kybernetickej bezpečnosti,
- záväzok a podporu vedenia,
- základný rámec riadenia rizík,
- základné postupy pre napĺňanie strategických cieľov,
- spôsob vyhodnocovania bezpečnostných cieľov.

Vypracovanie kontinuity činností v zmysle ZoKB

Zavedenie BCM umožní:

- Zabezpečiť dostupnosť kritických aktív a systémov v krízových situáciách v minimálnom možnom čase a s minimálnymi nákladmi
- Zaviesť prípravu a testovanie plánov obnovy prevádzkovaných IS s ohľadom na vnútorné procesy
- Efektívne zaistiť kontinuitu procesov, čo v prípade krízovej situácie prispeje k zníženiu finančných nákladov spojených s obnovou informačnej infraštruktúry a významne eliminuje finančné straty spôsobené jej nedostupnosťou

Zabezpečenie pozície manažéra kybernetickej bezpečnosti

Táto osoba by mala mať na starosti komplexné riadenie bezpečnosti v organizácii. Mala by spĺňať nielen odborné, ale aj osobnostné požiadavky, ktoré sú na túto rolu kladené. Túto rolu zabezpečíme dočasne externými kapacitami. Medzi základné úlohy manažéra kybernetickej bezpečnosti patria:

- Riadenie bezpečnosti,
- Manažment hrozieb a rizík
- Aplikácia bezpečnostných opatrení
- Výkon operatívnych bezpečnostných činností
- Riadenie súladu

Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti

Implementácia softvérového riešenia na monitorovanie dostupných technologických kapacít dôležitých sieťových zariadení a služieb podľa nakonfigurovaných pravidiel umožní v dostatočnom časovom predstihu upozorniť žiadateľa na dosahovanie limitu normovanej kapacity zariadení (napr. voľný priestor na HDD, maximálnu kapacitu servera a pod.). Takýmto spôsobom bude možné zaistiť riadenú a monitorovanú údržbu informačnej infraštruktúry žiadateľa bez rizika jej výpadku resp. obmedzenia prevádzky.

Nasadenie Next-Gen firewallu na perimeter siete

Firewall bude plniť funkcionalitu bezpečného oddelenia Internetu a vnútorných sietí. Bude zahŕňať funcionalitu NAT/PAT, zabezpečovať blokovanie nežiadúcej komunikácie na základe blokovania nežiadúcich webových stránok a aplikácií a taktiež ako antimalvérová ochrana. Aj smerovanie z užívateľských sietí do serverových sietí by malo byť smerované cez sieťový firewall a mali by byť povolené len tie služby, ktoré sú pre užívateľov nevyhnutné. Na perimetrovom firewalle budú blokované všetky neoprávnené spojenia z vonkajších sietí na vnútorné siete, ale aj opačne.

Modernizácia zálohovacieho systému

Prevádzka informačných systémov s dôrazom na ich spoľahlivosť, dostupnosť a vysokú bezpečnosť je hlavným cieľom navrhovaného technického riešenia. Vytvorenie efektívneho systému zálohovania, ktorý bude okrem iného schopný:

- Zabezpečiť takmer okamžitú ochranu dát zdieľaných zložiek
- Obnovu dát na úrovni súborov a zložiek s obnovením konkrétnych súborov alebo zložiek
- Zabezpečiť automatické opravy súborov napr. pomocou zrkadlených metadát a konfiguráciou RAID
- Zabezpečiť zálohovanie bez licencií určených k ochrane počítačov a serverov so systémom Windows, virtuálnych počítačov, ďalších súborových serverov a cloudových aplikácií
- Zabezpečiť konsolidáciu úloh zálohovania pre fyzické i virtuálne prostredie s možnosťou rýchleho obnovenia súborov, celých fyzických počítačov a virtuálnych počítačov umožní dosiahnuť požadovanú úroveň zálohovania dát, ktorá v prípade potreby bude schopná bez problémov obnoviť stratené dáta

Veľmi dôležitou výhodou zvýšenia kapacity zálohovacích systémov je bezpochyby aj možnosť vybudovania záložnej serverovne pre umiestnenie záložných systémov a kópie zálohovaných dát.

Kombinácia vyššie uvedených technických riešení umožní vytvoriť efektívnu správu IT infraštruktúry a zvýši ochranu kybernetického priestoru žiadateľa vyhovujúcu požiadavkám platnej legislatívy. Bližšie technické špecifikácie navrhovaných riešení sa nachádzajú v nasledujúcej časti Žiadosti o nenávratný finančný príspevok.

3.2.4 Rozsah projektu

Realizácia projektu sa dotkne nasledovných ISVS prevádzkovaných na úrovni TUZVO:

- isvs_14317-Elektronická registratúra TUZVO
- isvs_14318-CMS web sidla TUZVO
- isvs_14319 -Prístupový systém TUZVO
- isvs_14316 -Univerzitný informačný systém UIS TUZVO

Realizácia projektu sa dotkne nasledovných subjektov:

- Technická univerzita vo Zvolene
- Interní zamestnanci univerzity
- Externí zamestnanci univerzity
- Študenti
- Podnikatelia - dodávateľsko-odberateľské vzťahy

3.2.5 Motivácia a obmedzenia pre dosiahnutie cieľov projektu

Hlavnou motiváciou je realizácia opatrení KIB definovaných v zákone o kybernetickej bezpečnosti a v zákone o ISVS. Primárne ide o tie opatrenia, ktoré vykazujú najväčší nesúlad s uvedenými právnymi normami a vyhláškou 362/2018 Z. z.. Vďaka realizácii týchto opatrení budú IS TUZVO chránené v maximálnej možnej miere pred kybernetickým incidentom, ktorý by mohol mať na poskytovanie služieb a prevádzku IS TUZVO nasledovný dopad:

Dopad kybernetického bezpečnostného incidentu v závislosti	**Kategória**	**Vysvetlenie**

§ 24 ods. 2 písm. a) zákona 69/2018 Z.z. Počet používateľov základnej služby zasiahnutých kybernetickým bezpečnostným incidentom.	I.	TUZVO disponuje systémami, ktorých výpadok zasiahne viac ako 25 000 užívateľov univerzity. To znamená študentov, zamestnancov a externých partnerov.
§ 24 ods. 2 písm. b) zákona 69/2018 Z.z. Dĺžka trvania kybernetického bezpečnostného incidentu (čas pôsobenia kybernetického bezpečnostného incidentu) a/alebo § 24 ods. 2 písm. c) zákona Geografické rozšírenie kybernetického bezpečnostného incidentu.	I.	TUZVO prevádzkuje systémy pre interný personál, vedeckých pracovníkov a študentov, kde škoda, ktorá nastane je v rozsahu nad 15 000 používateľov.
§ 24 ods. 2 písm. d) zákona 69/2018 Z.z. Stupeň narušenia fungovania základnej služby.	II I.	V prípade nefunkčnosti informačných systémov nie je k dispozícii náhradné riešenie.
§ 24 ods. 2 písm. e) zákona 69/2018 Z.z. Rozsah vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu	I.	Incident spôsobí škody, ktoré má/môže mať dopad na viac ako 25 000 osôb. V prípade napadnutia a uniku osobných dát, informáciách o postavení, platových podmienkach a krádeže Know how a vedeckých výskumov, by boli škody veľmi veľké a možno aj fatálne. Nefunkčnosť systémov má priamy vplyv na hospodárske alebo spoločenské činnosti. Nefunkčnosť ISVS má priamy súvis na finančné operácie medzi univerzitou a dodávateľmi, odberateľmi, štátnymi inštitúciami (napr. sociálne a zdravotné poisťovne, daňový úrad...). Úspešný kybernetický útok, ktorého cieľom by bolo získanie dát z univerzity môže viesť a pravdepodobne aj bude viesť k úniku osobných údajov a následnému porušeniu práv dotknutých osôb. Vzhľadom na znenie §104 zákona č.: 18/2018 Z. z. a obdobné sankcie uvedené v GDPR môže vzniknúť škoda univerzite až do výšky 20 mil. €. Vychádzajúc z praxe a známych prípadov porušenia zákona na ochranu osobných údajov na území Slovenska môže takto jednému užívateľovi ISVS vzniknúť škoda prevyšujúca 250 000 €.

Projekt je formulovaný tak, aby po jeho realizácii nastal čo najväčší súlad zabezpečenia kybernetickej a informačnej bezpečnosti so zákonom o kybernetickej bezpečnosti a so zákonom o ISVS.

Obmedzenia projektu

Z hľadiska technického, personálneho, odborného, ale ani legislatívneho neevidujeme žiadne obmedzenia, ktoré by mohli ovplyvniť úspešnú realizáciu projektu.

3.3 Zainteresované strany/Stakeholder

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Univerzita - Administrátor IT	TUZVO	Vlastník procesu/ vlastník dát/ prevádzkovateľ / Užívateľ IS Zabezpečuje prevádzku IT	isvs_14317-Elektronická registratúra TUZVO isvs_14318-CMS web sidla TUZVO isvs_14319 -Prístupový systém TUZVO isvs_14316 -Univerzitný informačný systém UIS TUZVO
2	Manažér kybernetickej bezpečnosti	TUZVO	Zodpovedný za KIB	isvs_14317-Elektronická registratúra TUZVO isvs_14318-CMS web sidla TUZVO isvs_14319 -Prístupový systém TUZVO isvs_14316 -Univerzitný informačný systém UIS TUZVO
3.	Zamestnanec	TUZVO	Využíva IS Uni	isvs_14317-Elektronická registratúra TUZVO isvs_14318-CMS web sidla TUZVO isvs_14319 -Prístupový systém TUZVO isvs_14316 -Univerzitný informačný systém UIS TUZVO
4.	Študent	TUZVO	Využíva IS Uni	isvs_14317-Elektronická registratúra TUZVO isvs_14318-CMS web sidla TUZVO isvs_14319 -Prístupový systém TUZVO isvs_14316 -Univerzitný informačný systém UIS TUZVO
5.	podnikateľ		Využíva služby prostredníctvom IS	isvs_14317-Elektronická registratúra TUZVO isvs_14318-CMS web sidla TUZVO isvs_14319 -Prístupový systém TUZVO isvs_14316 -Univerzitný informačný systém UIS TUZVO
6.	Poskytovateľ IT služieb		Poskytuje služby IS	isvs_14317-Elektronická registratúra TUZVO isvs_14318-CMS web sidla TUZVO isvs_14319 -Prístupový systém TUZVO isvs_14316 -Univerzitný informačný systém UIS TUZVO

3.4 Ciele projektu

Ciele projektu sú definované v súlade s Národnou koncepciou informatizácie verejnej správy (ďalej len „NKIVS“) a súčasne sú definované tak, aby boli v súlade s očakávanými výsledkami definovanými v Partnerskej dohode Slovenskej republiky na roky 2021 – 2027 (ďalej len „Partnerská dohoda“) pre špecifický cieľ RSO 1.2. Definície cieľov rovnako vychádzajú z národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025.

Partnerská dohoda definuje špecifický cieľ RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy a konkrétne opatrenie: 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie, oblasť - Kybernetická a informačná bezpečnosť, pričom hlavným cieľom podpory je aj zabezpečenie kybernetickej bezpečnosti v súlade so Stratégiou digitálnej transformácie Slovenska. Stratégia digitálnej transformácie v oblasti kybernetickej bezpečnosti odkazuje na Národnú stratégiu kybernetickej bezpečnosti vydanú Národným bezpečnostným úradom (ďalej len „NBÚ“)

Národná koncepcia informatizácie verejnej správy určuje v rámci prioritnej osi 4 Kybernetická a informačná bezpečnosť strategickú prioritu Kybernetická a informačná bezpečnosť. Splnenie tejto strategickej priority má byť dosiahnuté nasledujúcimi dvoma cieľmi:

Cieľ 4.1 Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe

Cieľ 4.2 Posilniť ľudské kapacity a vzdelávanie v oblasti kybernetickej a informačnej bezpečnosti patriace pod prioritnú os 4 Kybernetická a informačná bezpečnosť.

Z vyššie uvedených cieľov je pre projekt dôležitý cieľ 4.1 a v súlade sním je aj nižšie citovaný strategický cieľ.

Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, ktorá vychádza z Partnerskej dohody definuje vo vzťahu k verejnej správe nasledovný strategický cieľ:

4.1 Dôveryhodný štát pripravený na hrozby.

V definícii tohto strategického cieľa uvádza, cit:

„Kybernetická bezpečnosť je zodpovednosťou každého obyvateľa Slovenskej republiky, no bezpečnosť nemôže fungovať bez existencie mechanizmov na národnej úrovni, ktoré určujú politiku kybernetickej bezpečnosti, systém jej riadenia, ale aj procesy na detekciu a riešenie kybernetických bezpečnostných incidentov, budovanie odborných kapacít a šírenie situačného a bezpečnostného povedomia. Zároveň štát musí pri budovaní dôveryhodnosti vykonávať vyššie uvedené aktivity v súlade s Ústavou Slovenskej republiky a ostatnými zákonmi a vstupovať do základných ľudských práv a slobôd len v nevyhnutnej miere.“

Cieľový stav uvedeného strategického cieľa je v Národnej stratégii kybernetickej bezpečnosti na roky 2021 až 2025 stanovený nasledovne, cit.:

„Vybudovanie dostatočného odborného personálneho základu pre systém riadenia informačnej a kybernetickej bezpečnosti nielen na národnej, ale aj sektorovej úrovni. Spolupráca štátu s občanom na úrovni poskytovania dostatočných informácií a odporúčaní a realizácia krokov, ktoré občan reálne pocíti ako zvýšenie vlastnej bezpečnosti a bezpečnosti národného kybernetického priestoru. Vytvorenie a používanie certifikačných schém na široké portfólio typov výrobkov, procesov a služieb. Kvalitnejšie technické, organizačné a personálne zabezpečenie, založené na využívaní moderných prístupov ku kybernetickej bezpečnosti pri detekcii a riešení kybernetických bezpečnostných incidentov. Vybudovanie spôsobilostí na detekciu a riešenie kybernetických bezpečnostných incidentov na všetkých úrovniach. Efektívna spolupráca zainteresovaných subjektov na všetkých úrovniach riešenia informačnej a kybernetickej bezpečnosti. Dobre nastavený proces technickej, ale aj politickej atribúcie kybernetických bezpečnostných incidentov. Systematické a kontinuálne riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch. Zlepšenie detekcie a zisťovania kybernetických bezpečnostných incidentov na sektorovej úrovni, zlepšenie a zjednodušenie nahlasovania kybernetických bezpečnostných incidentov nielen zo strany povinných subjektov, ale aj v rovine dobrovoľných hlásení. Podpora spôsobilostí subjektov v oblasti riadenia kontinuity činností.“

Hlavným cieľom je do prostredia univerzity v zaviesť optimalizáciu procesov riadenia kybernetickej bezpečnosti, riadenie rizík, kontinuity činností a riadenie incidentov pomocou finančných prostriedkov z dopytovej výzvy „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy“. Po implementácii projektu bude proces zavedený a ďalej vykonávaný aj internými zamestnancami, predovšetkým manažérom kybernetickej bezpečnosti, manažérom informačnej bezpečnosti a ďalšími bezpečnostnými zamestnancami. Hlavným výsledkom realizácie projektu bude realizácia a optimalizácia procesov riadenia kybernetickej bezpečnosti, riadenia rizík, kontinuity činností a riadenia incidentov.

Všetky ciele projektu sú definované v súlade s vyššie uvedenými strategickými dokumentmi:

ID	Názov cieľa	Názov strategického cieľa*	Spôsob realizácie strategického cieľa
1	Vytvorenie katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach Cieľ realizovaný v zmysle oprávnených podaktivít: - Riadenie rizík	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Vypracovanie a aktualizácia stratégie kybernetickej bezpečnosti a bezpečnostnej dokumentácie s prihliadnutím na štruktúru bezpečnostnej dokumentácie podľa prílohy č.1 vyhlášky 362/2018 Z.z. Vypracovaná dokumentácia bude pokrývať všetky požadované oblasti požadovanej legislatívy. Vypracovaný bude katalóg informačných aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovaný bude katalóg hrozieb a rizík a na základe týchto katalógov bude vypracovaná analýza rizík pre jednotlivé aktíva. Kompletná identifikácia informačných aktív organizácie, vytvorenie katalógu aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovanie zoznamu hrozieb a ohodnotenie dopadov na aktíva z pohľadu triády CIA. Vypracovanie smernice pre riadenie rizík, podľa ktorej bude vykonávaná analýza rizík informačných systémov univerzity.

2	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Cieľ realizovaný v zmysle oprávnených podaktivít: - Organizácia kybernetickej a informačnej bezpečnosti - Personálna bezpečnosť - Riadenie prístupov - Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami - Bezpečnosť pri prevádzke informačných systémov a sietí - Hodnotenie zraniteľností a bezpečnostné aktualizácie - Ochrana proti škodlivému kódu - Sieťová a komunikačná bezpečnosť - Zaznamenávanie udalostí a monitorovanie - Fyzická bezpečnosť a bezpečnosť prostredia - Riešenie kybernetických bezpečnostných incidentov - Kryptografické opatrenia - Audit a kontrolné činnosti	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z. Vypracovanie bezpečnostnej politiky pre univerzitu ohľadom riadenia, kontroly a vyhodnocovania stavu kybernetickej bezpečnosti na univerzite. Jedná sa o dokumentáciu, ktorá nie je zahrnutá v jednotlivých kapitolách - stratégia, bezpečnostná politika,... Vypracovanie bezpečnostného projektu pre systém Memphis, ktorý spadá pod ISVS. Vypracovanie postupov pri nástupe a odchode zamestnanca primárne z pohľadu prideľovania a odoberania prístupov do informačných systémov univerzity. Vypracovanie smernice pre koncových užívateľov a administrátorov, podľa ktorej sa bude riadiť bezpečnosť pri narábaní s pridelenými výpočtovými prostriedkami a pri prístupe do informačných systémov univerzity. Vypracovanie smernice pre riadenie prideľovania bezpečnostných rolí a úrovní prístupov pre interných a externých zamestnancov z dôvodu umožnenia prístupu k informačným systémom univerzity. Určenie a revízia dodávateľských zmlúv s tretími stranami, ktoré majú vplyv na poskytovanie kritických systémov organizácie. Návrh zmien v zmluvách týkajúcich sa oblasti kybernetickej bezpečnosti. Vypracovanie návrhu dodatku k zmluve s treťou stranou, ktorý bude pokrývať požiadavky ZoKB, ktoré sa týkajú dodávateľských vzťahov. Vypracovanie smernice pre administrátorov, podľa ktorej sa budú riadiť pri správe interných systémov univerzity. Vypracovanie postupov pre aplikovanie zmien v informačných systémoch univerzity a smerníc pre zaznamenávanie prevádzkových a bezpečnostných nastavení systémov. Vypracovanie interného riadiaceho dokumentu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat. Vypracovanie smernice na určenie zodpovednosti používateľov. Vypracovanie interného riadiaceho dokumentu pre administrátorov ohľadom ochrany koncových bodov pred škodlivým kódom. Vypracovanie interného riadiaceho dokumentu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti Vypracovanie dokumentácie spôsobu monitorovania a fungovania centrálneho log manažment systému a centrálneho nástroja na bezpečnostné monitorovanie a zadefinovanie spôsobu evidencie prevádzkových záznamov, ich vyhodnocovania, spôsobu hlásenia podozrivej aktivity, zodpovednej osoby a ďalších povinností. Vypracovanie smernice pre fyzickú a objektovú bezpečnosť, ktorá bude definovať požiadavky na zabezpečené priestory a na prístup do týchto priestorov. Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností, vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov. Vypracovanie smernice pre kryptografické opatrenia, ktorá bude definovať používanie a uchovávanie informácií týkajúcich sa použitých prístupových hesiel a kľúčov, bezpečnostných cetifikátov a ostatných bezpečnostných prvkov. Vypracovanie smernice pre posudzovanie bezpečnosti informačných systémov verejnej správy a ich vyhodnocovania.
3	Implementácia technických riešení podporujúcich riadenie bezpečnosti pri prevádzke Cieľ realizovaný v zmysle oprávnených podaktivít: - Bezpečnosť pri prevádzke informačných systémov a sietí	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia nástroja pre riadenie, evidenciu a schvaľovanie zmien, evidenciu bezpečnostných incidentov, konfiguračný manažment bezpečnostných nastavení.

4	Zvýšenie sieťovej a komunikačnej bezpečnosti nasadením a implementáciou NGFW do siete Cieľ realizovaný v zmysle oprávnených podaktivít: - Sieťová a komunikačná bezpečnosť	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia a konfigurácia perimetrového firewallu za účelom zabezpečenia bezpečného oddelenia internej siete a internetu. Úlohou tohto firewallu bude aj riešiť bezpečný prestup medzi segmentami siete a taktiež bude zabezpečovať bezpečný vzdialený prístup do siete na základe VPN spojení s overovaním pomocou dvojfaktorovej autentizácie. Zariadenia budú poskytovať pokročilé funkcie ako hĺbková inšpekcia sieťovej prevádzky, detekcia a prevencia hrozieb.
5	Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity Cieľ realizovaný v zmysle oprávnených podaktivít: - Sieťová a komunikačná bezpečnosť	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia dohľadového nástroja, ktorý sleduje a identifikuje sieťové spojenia na hranici s vonkajšou sieťou, vytvára prehľady o prenesených dátach, o podozrivých prístupoch na škodlivé stránky a je schopný vytvárať automatizované reporty z pohľadu dodržiavania bezpečnostných smerníc. Zakúpenie a implementácia nástroja na sledovanie interných dátových tokov pomocou zrkadlenia prevádzky za účelom identifikácie dátových tokov medzi jednotlivými zariadeniami v sieti s funkcionalitou deep-packet-inspection za účelom odhaľovania anomálií v sieťovej prevádzke. Implementácia a konfigurácia nástroja určeného na bezpečnostný dohľad internej komunikácie v sieti na základe deep packet inspection, Na základe sledovania a detegovania podozrivej komunikácie bude možné na základe behaviorálnej analýzy odhaliť podozrivú aktivitu, resp. prienik na servery a systémy, ktoré podporujú základné služby organizácie.
6	Implementácia centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov Cieľ realizovaný v zmysle oprávnených podaktivít: - Sieťová a komunikačná bezpečnosť	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Zakúpenie a implementácia zariadenia pre centrálny zber systémových logov z rôznych zariadení a systémov prevádzkovaných v sieti univerzity. Vypracovanie pravidiel pre nasadenie logovania na rôzne zariadenia a vytvorenie korelačných pravidiel za účelom notifikovania administrátorov ohľadom podozrivých aktivít v sieti a na systémoch. Implementácia SIEM nástroja pre koreláciu dát a informácií z rôznych zdrojov za účelom generovania alertov a vytvárania incidentov za účelom ich evidencie a evidencie postupov riešenia.
7	Implementácia systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov. Cieľ realizovaný v zmysle oprávnených podaktivít: - Sieťová a komunikačná bezpečnosť		Implementácia dohľadového systému na sledovanie prevádzkových parametrov siete a systémov. Ide primárne o sledovanie dostupnosti jednotlivých zariadení, systémov a služieb a o sledovanie vyťaženosti systémov a služieb na týchto systémoch. Vytvorenie a zadefinovanie hraničných parametrov tak, že pri ich prekročení budú administrátori notifikovaní o vzniknutí tejto udalosti.
8	Implementácia nástroja na centrálne riadenie ochrany pred škodlivým kódom Cieľ realizovaný v zmysle oprávnených podaktivít: - Ochrana proti škodlivému kódu	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia nástroja na centrálne riadenie ochrany pred škodlivým kódom. Bude nasadený nástroj na riadenie aktualizácií na koncových zariadeniach a taktiež bude nakonfigurovaný systém pre centrálnu správu antivírového systému.

9	Zavedenie nástroja určeného na notifikovanie o existujúcich zraniteľnostiach programových prostriedkov a ich častí Cieľ realizovaný v zmysle oprávnených podaktivít: - Hodnotenie zraniteľností a bezpečnostné aktualizácie	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia a konfigurácia nástroja, ktorý bude automaticky informovať administrátorov systémov v prípade výskytu novej zraniteľnosti na základe prístupov do databáz známych zraniteľností.
10	Zvýšenie bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít Cieľ realizovaný v zmysle oprávnených podaktivít: - Kontinuita prevádzky	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia zabezpečeného systému zálohovania vo fyzicky oddelenej budove za účelom zabezpečenia kópie dôležitých systémov a dát v prípade zlyhania alebo zničenia primárnej serverovne. Systém zálohovania by mal mať ochranu pred zmazaním a prepísaním uložených dát a mal by uchovávať zálohy v šifrovanej podobe. Zaobstaranie licencií potrebných pre úspešné prevádzkovanie bezpečného zálohovania dôležitých systémov a dát.
11	Vypracovanie plánov kontinuíty a ich otestovanie Cieľ realizovaný v zmysle oprávnených podaktivít: - Kontinuita prevádzky	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Vypracovanie stratégie a krízových plánov pre dva kritické systémy univerzity v prevádzke na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu. Vypracovanie dekompozície dôležitých služieb a vypracovanie BIA pre tieto služby, resp. systémy. Vypracovanie plánov kontinuity prevádzky a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania.
12	Implementácia systému pre inventarizáciu aktív Cieľ realizovaný v zmysle oprávnených podaktivít: - Riadenie rizík	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Implementácia jednotného informačného systému KB. Návrh interného systému na riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík s ohľadom na aktívum, určenie vlastníka rizika, implementácie organizačných a technických bezpečnostných opatrení, analýzy funkčného dopadu a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení"

* Definícia strategického cieľa vychádza zo strategického cieľa v Národnej stratégii kybernetickej bezpečnosti a nadväzuje na prioritný cieľ Národnej koncepcie informatizácie verejnej správy.

3.5 Merateľné ukazovatele (KPI)

ID	ID /Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
1	PO 095 / PS KPS OI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy.	Verejné inštitúcie	0	1	Identifikácia počtu realizácie opatrení KIB pre inštitúciu – splnenie súladu KIB so zákonom o kybernetickej bezpečnosti a zákonom o ISVS Čas plnenia merateľného ukazovateľa projektu: Fyzické ukončenie realizácie hlavných aktivít projektu	Typ ukazovateľa: Výstup
	PR 017 / PS KPR CR 11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Užívatelia / rok	0	2400	Sumarizácia počtu používateľov nových a vylepšených digitálnych služieb – bude určené počtom prístupov v IAM, Databázou používateľov v oblasti KIB. V prípade univerzity ide o počet používateľov, ktorí priamo využívajú IS a priamo sa podieľajú na zabezpečovaní základnej služby. Čas plnenia merateľného ukazovateľa projektu: v rámci udržateľnosti projektu	Typ ukazovateľa: výsledok

3.5.1 Špecifikácia potrieb koncového používateľa

Z pohľadu TUZVO je koncovým používateľom IT oddelenie a sekundárne zamestnanci TUZVO a študenti, ktorí očakávajú, že nebude vplyvom kybernetických útokov dochádzať k výpadkom prevádzky IS univerzity a tým sa de facto znefunkční poskytovanie univerzitných služieb.

TUZVO plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním nasledovných krokov:

- vytvorením katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach,
- vytvorením, resp. aktualizovaním kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.,
- implementáciou technických riešení podporujúcich riadenie bezpečnosti pri prevádzke,
- implementáciou systému na nepretržitú kontrolu dátových tokov v interných sieťach univerzity,
- implementáciou automatického nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou,
- implementáciou centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov,
- implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov,
- Implementáciou nástroja na centrálne riadenie ochrany pred škodlivým kódom
- implementáciou nástroja na detekciu, nástroja na zber a nepretržité vyhodnocovanie a evidenciu kybernetických bezpečnostných udalostí,
- zavedením nástroja určeného na notifikovanie o existujúcich zraniteľnostiach programových prostriedkov a ich častí,
- zvýšením bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít,
- vypracovaním plánov kontinuity a ich otestovaním,
- implementáciou systémov na správu a inventarizáciu aktív,

Predmet plnenia

1.Organizácia kybernetickej a informačnej bezpečnosti

- Vypracovanie bezpečnostnej politiky pre univerzitu ohľadom riadenia, kontroly a vyhodnocovania stavu kybernetickej bezpečnosti na univerzite.
- Vypracovanie bezpečnostného projektu pre systém Memphis, ktorý spadá pod ISVS.
- Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z. Vypracovaná dokumentácia bude pokrývať všetky požadované oblasti požadovanej legislatívy. Pri vypracovávaní dokumentácie sa bude vychádzať z metodík vydaných MIRRI.

2. Riadenie rizík

- Kompletná identifikácia informačných aktív univerzity, vytvorenie katalógu aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovanie zoznamu hrozieb a ohodnotenie dopadov na aktíva z pohľadu triády CIA.
- Vypracovaný bude katalóg informačných aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovaný bude katalóg hrozieb a rizík a na základe týchto katalógov bude vypracovaná analýza rizík pre jednotlivé aktíva.
- Implementácia informačného systému určeného pre identifikáciu, analýzu a riadenie rizík v organizácii. RIA IS a ALVAO Asset Management
- Vypracovanie smernice pre riadenie rizík, podľa ktorej bude vykonávaná analýza rizík informačných systémov univerzity

3. Personálna bezpečnosť

    - Vypracovanie postupov pri nástupe a odchode zamestnanca primárne z pohľadu prideľovania a odoberania prístupov do informačných systémov univerzity.
    - Vypracovanie smernice pre koncových užívateľov a administrátorov, podľa ktorej sa bude riadiť bezpečnosť pri narábaní s pridelenými výpočtovými prostriedkami a pri prístupe do informačných systémov univerzity.

4. Riadenie prístupov

- Vypracovanie smernice pre riadenie prideľovania bezpečnostných rolí a úrovní prístupov pre interných a externých zamestnancov z dôvodu umožnenia prístupu k informačným systémom univerzity

5. Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami

- Určenie a revízia dodávateľských zmlúv s tretími stranami, ktoré majú vplyv na poskytovanie kritických systémov organizácie. Návrh zmien v zmluvách týkajúcich sa oblasti kybernetickej bezpečnosti.
- Vypracovanie návrhu dodatku k zmluve s treťou stranou, ktorý bude pokrývať požiadavky ZoKB, ktoré sa týkajú dodávateľských vzťahov.

6. Bezpečnosť pri prevádzke informačných systémov a sietí

- Analýza a návrh pravidiel a politík pre koncové stanice v závislosti od ich použitia. Činnosť pozostáva z identifikácie use cases a návrhu na optimálne zabezpečenie identifikovaných kategórií pracovných staníc (učebne – študentské, prezentačné PC, zamestnanci pedagogickí, administratívni).
- Vypracovanie smernice pre administrátorov, podľa ktorej sa budú riadiť pri správe interných systémov univerzity. Vypracovanie postupov pre aplikovanie zmien v informačných systémoch univerzity a smerníc pre zaznamenávanie prevádzkových a bezpečnostných nastavení systémov.
- Implementácia nástroja Alvao Service Desk pre riadenie, evidenciu a schvaľovanie zmien, evidenciu bezpečnostných incidentov, konfiguračný manažment bezpečnostných nastavení.
- Implementácia a konfigurácia monitorovacieho nástroja, ktorý bude monitorovať prevádzkové parametre prevádzkovaných systémov a ktorý bude alertovať v prípade, že dôjde k odchýlke týchto parametrov od bežnej prevádzky.

7. Hodnotenie zraniteľností a bezpečnostné aktualizácie

- Implementácia a konfigurácia nástroja, ktorý bude automaticky informovať administrátorov systémov v prípade výskytu novej zraniteľnosti na základe prístupov do databáz známych zraniteľností.
- Inštalácia servera podľa požiadaviek aplikácie a konfigurácie systému pre notifikáciu zraniteľností v kritických systémoch.
- Vypracovanie interného riadiaceho dokumentu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat.

8. Ochrana proti škodlivému kódu

- Vypracovanie smernice ohľadom implementácie a správy systémov, ktoré majú za úlohu chrániť organizáciu pred škodlivým kódom.
- Implementácia a zdokumentovanie nasadenia centrálneho riadenia v súčasnosti nasadeného riešenia ESET pre ochranu pred škodlivým kódom.
- Vypracovanie interného riadiaceho dokumentu pre administrátorov ohľadom ochrany koncových bodov pred škodlivým kódom

9. Sieťová a komunikačná bezpečnosť

- Implementácia a konfigurácia perimetrového firewallu za účelom zabezpečenia bezpečného oddelenia internej siete a internetu. Úlohou tohto firewallu bude aj riešiť bezpečný prestup medzi segmentami siete a taktiež bude zabezpečovať bezpečný vzdialený prístup do siete na základe VPN spojení s overovaním pomocou dvojfaktorovej autentizácie
- Vypracovanie interného riadiaceho dokumentu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti
- Implementácia dohľadového nástroja, ktorý sleduje a identifikuje sieťové spojenia na hranici s vonkajšou sieťou, vytvára prehľady o prenesených dátach, o podozrivých prístupoch na škodlivé stránky a je schopný vytvárať automatizované reporty z pohľadu dodržiavania bezpečnostných smerníc.
- Implementácia samostatného hardvérového a konfigurácia nástroja určeného na bezpečnostný dohľad internej komunikácie na základe deep packet inspection, ktorý bude sledovať primárne komunikáciu interných zamestnancov na serverovú infraštruktúru univerzity. Na základe sledovania a detegovania podozrivej komunikácie bude možné na základe behaviorálnej analýzy odhaliť podozrivú aktivitu, resp. prienik na servery a systémy, ktoré podporujú základné služby univerzity

10. Zaznamenávanie udalostí a monitorovanie

- Zaobstaranie, implementácia a konfigurácia centrálneho logovacieho systému, ktorý bude bezpečným spôsobom zbierať, vyhodnocovať, vizualizovať a ukladať systémové logy zo všetkých dôležitých systémov univerzity

- Nastavenie požadovaných alertov z centrálneho logovacieho systému, ktoré budú na základe korelačných pravidiel vytvárať alerty v prípade vzniku podozrivej aktivity na logovaných systémoch
- Vypracovanie dokumentácie spôsobu monitorovania a fungovania centrálneho log manažment systému a centrálneho nástroja na bezpečnostné monitorovanie a zadefinovanie spôsobu evidencie prevádzkových záznamov, ich vyhodnocovania, spôsobu hlásenia podozrivej aktivity, zodpovednej osoby a ďalších povinností
- Implementácia a konfigurácia monitorovacieho nástroja, ktorý bude monitorovať prevádzkové parametre prevádzkovaných systémov a ktorý bude alertovať v prípade, že dôjde k odchýlke týchto parametrov od bežnej prevádzky.
- Tento cieľ bude naplnený implementáciou pohľadového systému pre sledovanie prevádzkových parametrov všetkých systémov podieľajúcich sa na prevádzke alebo podpore poskytovaných služieb: sieťových zariadení, serverov, aplikácií a ďalších IT prostriedkov. Robustná open-source platforma určená na monitorovanie sietí, serverov a aplikácií. Jeho hlavnou úlohou je poskytovať komplexný prehľad o výkone a dostupnosti vašej IT infraštruktúry v reálnom čase, čo umožňuje efektívne predchádzať problémom skôr, než negatívne ovplyvnia chod IKT. Systém musí podporovať široké spektrum metód na zber dát vrátane agentov, SNMP, IPMI, JMX, trapy a log súbory, čo zaručí flexibilitu a kompatibilitu s rôznymi zariadeniami a aplikáciami. V prípade potreby musí byť možné využiť proxy, ktorý zníži záťaž na hlavný server a umožní efektívne monitorovanie geograficky vzdialených lokalít.
- Kľúčové požadované vlastnosti:
    - konfigurovateľné upozornenia a notifikácie, ktoré môžu byť zasielané prostredníctvom emailov, SMS, skriptov alebo webhookov,
    - vizualizácia dát pomocou grafov, máp, prehľadov a dashboardov,
    - šifrovaná komunikácia medzi serverom, agentmi a užívateľom, čo zaručuje ochranu citlivých informácií,
    - podpora autentifikácie a rôznych úrovní prístupových práv zabezpečí, že prístup k monitorovacím dátam budú len oprávnené osoby.

11. Fyzická bezpečnosť a bezpečnosť prostredia

- Vypracovanie smernice pre fyzickú a objektovú bezpečnosť, ktorá bude definovať požiadavky na zabezpečené priestory a na prístup do týchto priestorov.

12. Riešenie kybernetických bezpečnostných incidentov

- Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností, vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov

13. Kryptografické opatrenia

- Vypracovanie smernice pre kryptografické opatrenia, ktorá bude definovať používanie a uchovávanie informácií týkajúcich sa použitých prístupových hesiel a kľúčov, bezpečnostných certifikátov a ostatných bezpečnostných prvkov

14. Kontinuita prevádzky

- Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu. Vypracovanie dekompozície dôležitých služieb a vypracovanie BIA pre tieto služby, resp. systémy
- Vypracovanie plánov kontinuity prevádzky pre dva kritické systémy univerzity a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania.
- Vykonanie testovania navrhnutých plánov kontinuity a zapracovanie nedostatkov z výsledkov testovania
- Implementácia zabezpečeného systému zálohovania vo fyzicky oddelenej budove za účelom zabezpečenia kópie dôležitých systémov a dát v prípade zlyhania alebo zničenia primárnej serverovne. Systém zálohovania by mal mať ochranu pred zmazaním a prepísaním uložených dát a mal by uchovávať zálohy v šifrovanej podobe
- Zaobstaranie licencií potrebných pre úspešné prevádzkovanie bezpečného zálohovania dôležitých systémov a dát
- Tento bod bude splnený dodávkou HW zariadení na ukladanie záložných kópií a taktiež dodávkou samostatných diskových úložísk za účelom vytvárania offline kópií zálohovaných systémov.
- V projekte by mali byť pokryté nasledujúce činnosti:
    - Dodávka hardvéru na ukladanie šifrovanej zálohy dát.
    - Realizácia inštalačných a konfiguračných služieb, ktoré zabezpečia možnosť ukladania zálohy prevádzkových dát, vrátane testovacej obnovy dát.
- Výsledný systém zálohovania na zabezpečenie kontinuity prevádzky bude mať nasledovné kľúčové prvky:
    - Dátový sklad musí byť navrhnutý a realizovaný tak, aby zabránil útočníkom v neoprávnenom zmenení alebo odstránení zálohovaných dát. To znamená, že raz uložené dáta nie sú zraniteľné voči zmenám alebo útokom, čím sa zabezpečuje ich dôveryhodnosť.
    - Musí byť vybavený mechanizmami na overenie a šifrovanie, čo zvyšuje bezpečnosť uložených dát. Digitálne podpisy a šifrovanie musia pomôcť pri zabezpečovaní integrity a dôvernosti dát.
    - Musí byť navrhnutý s dôrazom na správne riadenie prístupu. To znamená, že iba oprávnené osoby alebo procesy by mali mať prístup k zálohovaným dátam, a to na základe princípu najnižších pridelených oprávnení.

15. Audit a kontrolné činnosti

- Vypracovanie smernice pre posudzovanie bezpečnosti informačných systémov verejnej správy a ich vyhodnocovania.

3.6 Riziká a závislosti

Zoznam rizík a závislostí je detailne rozpracovaný v prílohe tohto dokumentu č. 1: Zoznam rizík a závislostí. Tento zoznam bude počas celej realizácie projektu aktualizovaný.

3.7 Stanovenie alternatív v biznisovej vrstve architektúry

Posudzovanie alternatív riešenia vychádza z viacerých možností. V prípade TUZVO, ktorá má zabezpečenú čiastočnú úroveň kybernetickej bezpečnosti prichádzajú do úvahy nasledovné 3 alternatívy:

1. Ponechanie existujúceho stavu – ide o nultý stav, v ktorom TUZVO spĺňa len čiastočné požiadavky na kybernetickú bezpečnosť a ide o možné ohrozenie IS TUZVO.
2. Realizácia projektu KIB s doplnením vybraných opatrení (t.j. nie všetkých) – došlo by k zvýšeniu súladu s legislatívou a s požiadavkami na technické zabezpečenie KB, ale informačné systémy univerzity by boli naďalej kriticky ohrozené.
3. Realizácia opatrení na dosiahnutie zvýšenia súladu KIB s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS – pôjde o také zvýšenie súladu s požiadavkami príslušnej legislatívy v oblasti KIB, ktorá zabezpečí ochranu TUZVO pred najväčšími hrozbami, pričom by šlo o in house riešenie (dohľad nad všetkými systémami vo vlastnej réžii TUVZO).
4. Realizácia opatrení na dosiahnutie zvýšenia súladu KIB s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS – pôjde o také zvýšenie súladu s požiadavkami príslušnej legislatívy v oblasti KIB, ktorá zabezpečí ochranu TUVZO pred najväčšími hrozbami a niektoré služby budú realizované ako externá služba (SIEM a SOC služby realizované ako služba).

Z hľadiska identifikovaných procesov v kapitole 3.5 alternatíva 1 nepokryje riešenie žiadneho z identifikovaných problémov.

V prípade čiastkového riešenia (alternatíva 2) by boli zvolené iba niektoré z procesov, ktoré by boli projektom vyriešené.

V prípade alternatívy 3 budú podporené všetky procesy v oblasti KIB, ktoré je potrebné pre účely ochrany IS, a ktoré zabezpečujú prevádzku TUZVO.

Alternatíva 4 rieši pokrytie všetkých procesov v oblasti KIB, ktoré sú potrebné pre účely ochrany IS, ale vyžadujú platbu externým subjektom minimálne počas doby udržateľnosti projektu.

Na základe zhodnotenia sa ukazuje ako najprijateľnejšia alternatíva možnosť 3, kedy dôjde k značnému zvýšeniu stavu KB na univerzite a nebude ohrozená udržateľnosť z dôvodu finančnej náročnosti.

3.8 Multikriteriálna analýza

Multikriteriálna analýza je v tomto prípade redukovaná na dva parametre:

1. Potrebu zosúladenia úrovne kybernetickej bezpečnosti s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS na maximálnu možnú dosiahnuteľnú úroveň. Táto požiadavka sa dotýka všetkých stakeholderov a predstavuje KO kritérium. Ak nemá dôjsť k zásadnému zvýšeniu kybernetickej a informačnej bezpečnosti TUZVO, t.j. ak má zostať ponechaný stav alebo iba dôjde k čiastočnému zlepšeniu, nebude možné považovať realizovaný projekt za úspešný.
2. Udržateľnosť riešenia.

Z vyššie uvedených možných alternatív vyplýva, že s ohľadom na potreby a finančné možnosti TUZVO v rámci udržateľnosti je najvýhodnejšia a dlhodobo udržateľná alternatíva 3.

3.9 Stanovenie alternatív v aplikačnej vrstve architektúry

HW a SW komponenty, rovnako ako služby, ktoré sú s nimi spojené musia zodpovedať požiadavkám definovaným v projekte koncovými používateľmi - tými sú v tomto prípade oddelenie informatiky, ktoré vychádza z požiadaviek zákona o kybernetickej bezpečnosti, zákona o ISVS, vyhlášky 362/2018 Z. z. a ďalších predpisov.

Aplikačná vrstva predpokladá dve alternatívy:

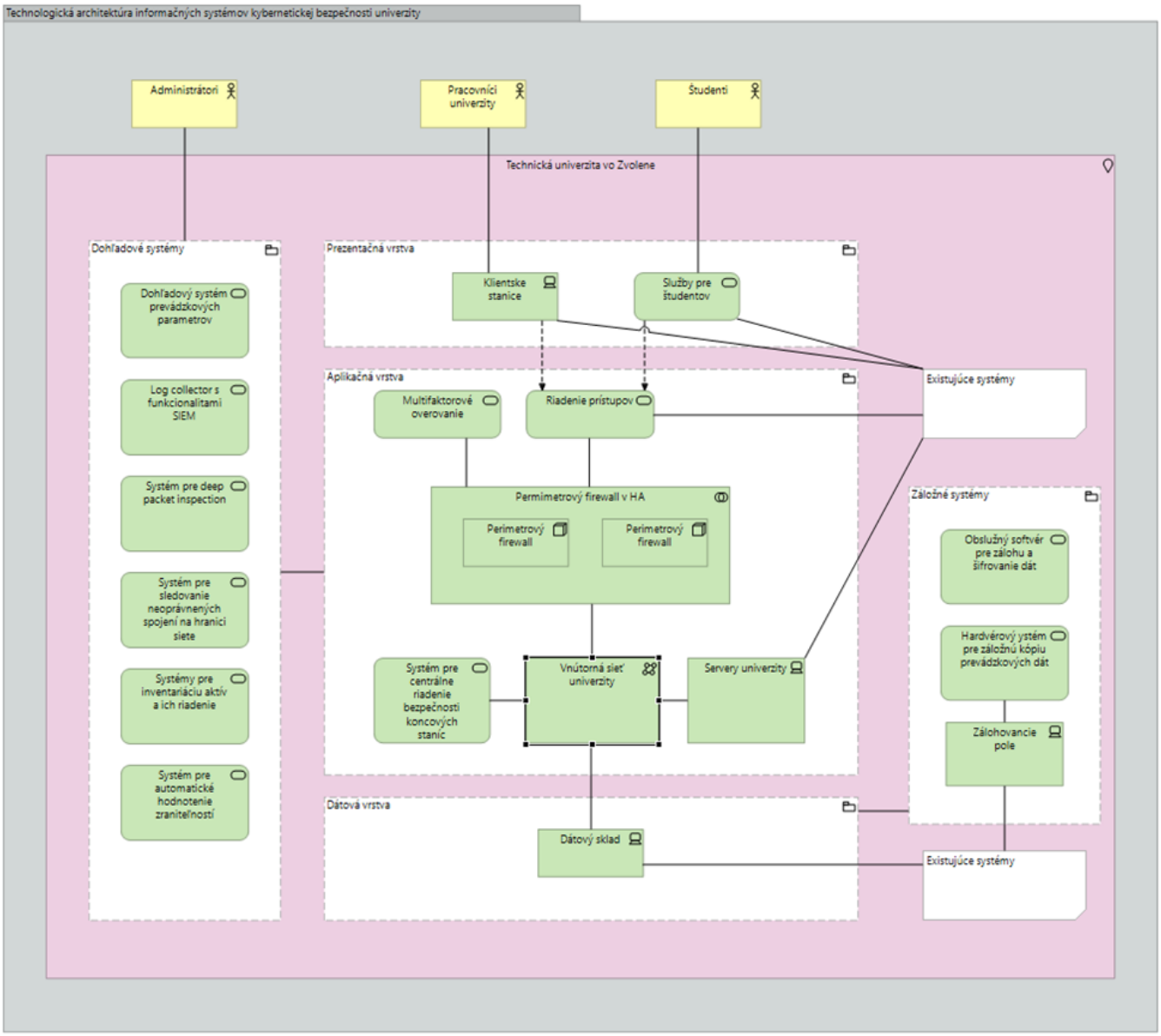
1. realizácia všetkých opatrení na úrovni TUZO v zmysle definovaných požiadaviek, pričom všetky technológie na realizáciu opatrení KIB budú vytvorené ako IN-HOUSE riešenie - táto architektúra zodpovedá alternatíve 3 popísanej v multikriteriálnej analýze
2. realizácia všetkých opatrení na úrovni TUZVO v zmysle definovaných požiadaviek, pričom niektoré technológie na realizáciu opatrení KIB budú vytvorené ako IN-HOUSE riešenie a niektoré ako služba, konkrétne SIEM - táto architektúra zodpovedá alternatíve 4 popísanej v multikriteriálnej analýze.

Aplikačne teda bude zvolená architektúra 1.

3.10 Stanovenie alternatív v technologickej vrstve architektúry

Z hľadiska použitých technológií nie sú definované alternatívy. Požiadavky na technológie sú definované všeobecne tak, aby ľubovoľnú SW a HW technológia, ktorá splní definované požiadavky koncového používateľa, bolo možné použiť na realizáciu projektu.

Technologickú architektúru riešenia definuje nasledovný obrázok:



4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Výsledkom projektu budú:

Projektové výstupy v zmysle vyhlášky 401/2023 o riadení projektov. V prípade, že predmetom realizácie bude dielo (oceniteľné práva a/alebo zdrojový kód), získa TUZVO právo vykonávať autorské práva k tomuto dielu, vrátane výhradnej a územne neobmedzenej licencie. Tieto podmienky sa nevzťahujú na tzv. krabicový softvér, ktorý je predávaný ako produkt či už realizátora alebo tretej strany.

Z hľadiska plnenia cieľov projektu bude výsledkom projektu naplnenie hlavného cieľa, t.j. súlad KIB so zákonom o kybernetickej bezpečnosti a so zákonom o ISVS, čo bude naplnené realizáciu nasledovných partikulárnych cieľov:

- Organizácia kybernetickej a informačnej bezpečnosti
- Riadenie rizík
- Personálna bezpečnosť
- Riadenie prístupov
- Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami
- Bezpečnosť pri prevádzke informačných systémov a sietí
- Hodnotenie zraniteľností a bezpečnostné aktualizácie
- Ochrana proti škodlivému kódu
- Sieťová a komunikačná bezpečnosť
- Zaznamenávanie udalostí a monitorovanie
- Fyzická bezpečnosť a bezpečnosť prostredia

- Riešenie kybernetických bezpečnostných incidentov
- Kryptografické opatrenia
- Kontinuita prevádzky
- Audit a kontrolné činnosti

Technologicky a administratívne pôjde o realizáciu nasledovných cieľov:

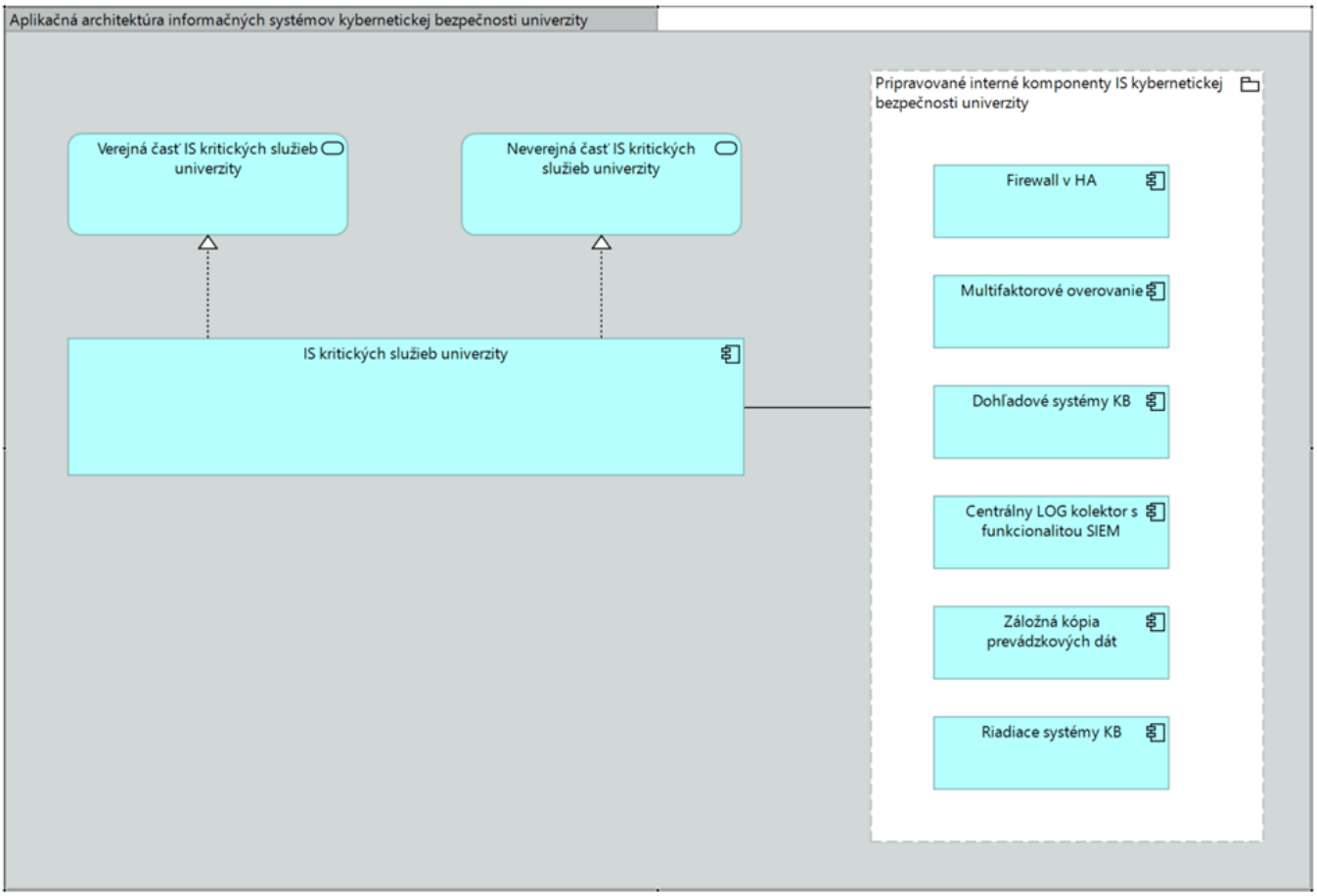
- Vytvorenie katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach
- Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.
- Implementácia technických riešení podporujúcich riadenie bezpečnosti pri prevádzke
- Zvýšenie sieťovej a komunikačnej bezpečnosti nasadením a implementáciou NGFW a segmentáciou siete
- Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity
- Implementácia centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov
- Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.
- Implementácia nástroja na centrálne riadenie ochrany pred škodlivým kódom
- Zavedenie nástroja určeného na notifikovanie o existujúcich zraniteľnostiach programových prostriedkov a ich častí
- Zvýšenie bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít
- Vypracovanie plánov kontinuíty a ich otestovanie
- Implementácia systémov na správu a inventarizáciu aktív

5. NÁHĽAD ARCHITEKTÚRY

Architektúra celého riešenia je v zmysle usmernenia MIRRI SR rámcová tak, aby bolo z projektu zrejmé, ktoré komponenty v rámci realizácie projektu budú vytvorené (a budú realizovať opatrenia KIB).

Primárne opatrenia kybernetickej bezpečnosti chránia IS TUZVO, ktoré sú určené na prevádzkovanie univerzitných služieb TUZVO. Z vyššie definovaných potrieb je zrejmé, o aké komponenty zabezpečenia pôjde - firewally, multifaktorové overovanie, centrálny logovací nástroj, nástroj na sledovanie prevádzkových parametrov siete, nástroje na detekciu v sieti a na hranici siete, nástroj na analýzu dátových tokov v sieti, systém na vyhodnocovanie kybernetických bezpečnostných udalostí a incidentov, centrálne riadenie záplat a aktualizácií, záložná kópia prevádzkových dát, kompletná dokumentácia podľa ZoKB vrátane BCM plánov.

Aplikačnú architektúru riešenia definuje nasledovný obrázok:



6. LEGISLATÍVA

V rámci platnej legislatívy nebude potrebné meniť žiadnu legislatívu. Projekt je realizovaný za účelom dosiahnutia súladu s platnou legislatívou a to najmä:

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS
- Vyhláška č.401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy
- Vyhláška 179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS
- Vyhláška 362/2018 Z.z. o obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení)

7. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

Harmonogram projektu je definovaný na základe odporúčania MIRRI SR, ktoré predpokladá trvanie projektu na úrovni približne jedného roka. S ohľadom na potreby nákupu a implementácie technológií vrátane potreby ich skúšobnej prevádzky sa s týmto časom stotožňujeme.

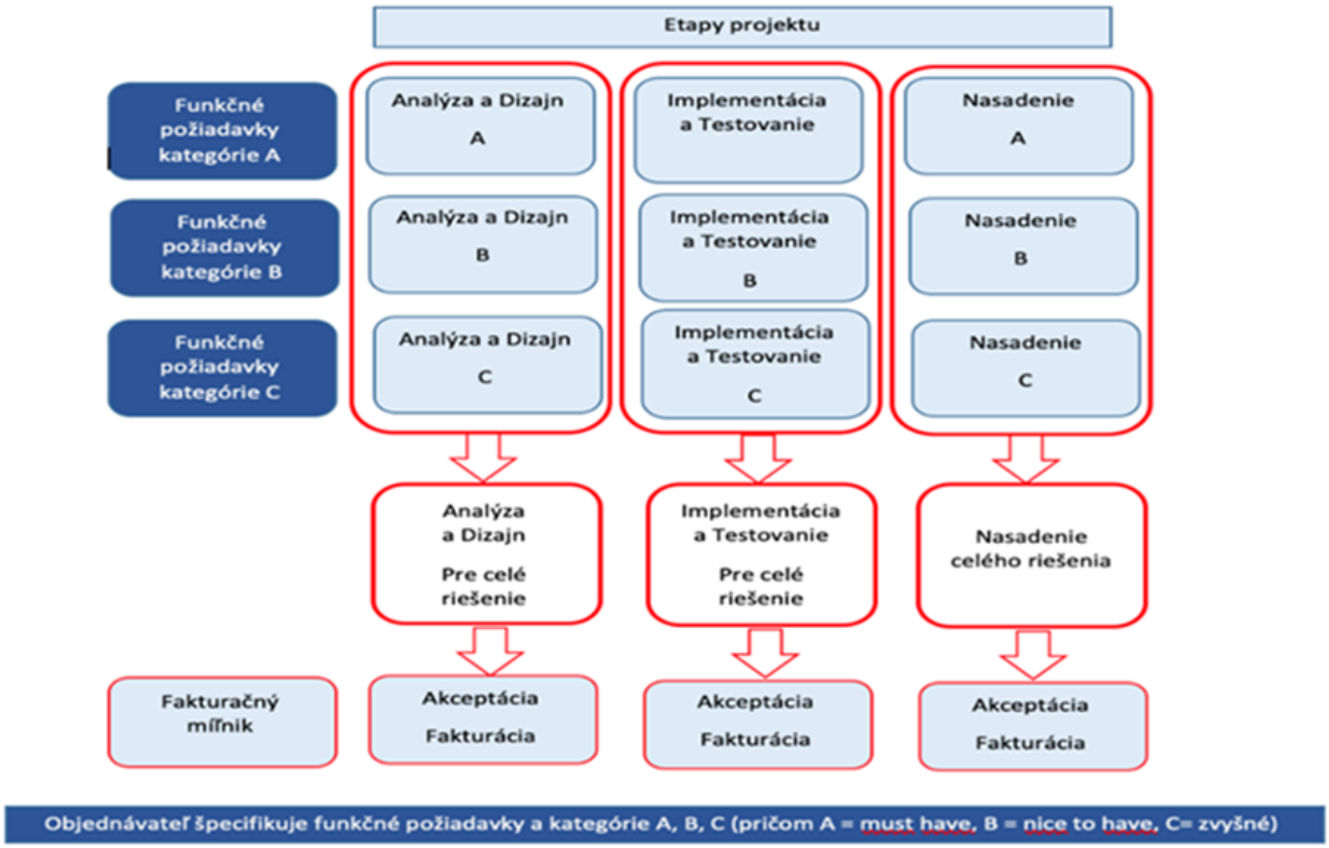
Začiatok realizačnej fázy projektu vyplýva z predpokladu, že realizácia projektu začne až po ukončení administratívneho a odborného hodnotenia a po podpise Zmluvy o NFP, pričom je definovaná dostatočná časová rezerva na tieto úkony. Rovnako na procesy verejného obstarávania, ktoré môžu potenciálne začať v krátkom čase po podaní žiadosti o NFP.

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza a Iniciačná fáza	4/2024	12 /2024	Podpísanie zmluvy o NFP Spustenie procesov VO
2.	Realizačná fáza			Podpísanie zmlúv s dodávateľmi po ukončení VO, realizácia

		01 /2025	11 /2025	
2a	Analýza a Dizajn	04 /2025	05 /2025	
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	04 /2025	08 /2025	
2c	Implementácia a testovanie	08 /2025	10/2025	Min. 2 mesiace test. prevádzky
2d	Nasadenie opatrení	10 /2025	11/2025	
3.	Dokončovacia fáza	10/2025	12/2025	Počas dokončovacej fázy projektový manažér pripraví podklady a odovzdá na schválenie záverečnú žiadosť o platbu a záverečnú monitorovaciu správu.
4.	Podpora prevádzky (SLA)	01/2026	01/2031	Obdobie udržateľnosti

Ako metóda riadenia projektu bude použitá metóda „Waterall“. Táto metóda sa ukázala byť ako najvhodnejšia nakoľko svojimi charakteristikami a možnosťami plne zodpovedá požiadavkám a predstavám univerzity.

Schéma metódy projektového riadenia:



8. ROZPOČET A PRÍNOSY

V uvedenom projekte vychádzame pri stanovení rozpočtu z prieskumu trhu a pravidiel stanovených výzvou. S ohľadom na rozpočet projektu (projekt do 1 000 000,00,- EUR) nebola spracovaná Analýza nákladov a prínosov.

8.1. Sumarizácia nákladov a prínosov

Náklady	Infraštruktúra pre prevádzku kybernetickej bezpečnosti	Dokumentácia KB	Pre všetky podaktivity

IT - CAPEX			
Aplikácie			
SW	118 392,00 €		
HW	141 081,60 €		
Práce/služby	18 480,00 €	57 000,07 €	
Mzdy interní zamestnanci			121 386,89 €
Paušálne výdavky			31943,84 €
IT - OPEX- prevádzka			
Aplikácie			
SW	35 836,80 €*		
HW			

***V Detailných informáciách projektu je uvedená suma 29 864 Eur, čo je 35 836,80 s DPH.**

8.2. Sumarizácia podľa podaktivít

Názov	HW	SW	Služby
1.Vytvorenie katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach			5 400,00 €
2.Vytvorenie, resp. aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.			33 600,07 €
3.Implementácia technických riešení podporujúcich riadenie bezpečnosti pri prevádzke		24 000,00 €	
4.Zvýšenie sieťovej a komunikačnej bezpečnosti nasadením a implementáciou NGFW do siete	17 328,00 €	11 520,00 €	
5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity	70 392,00 €	1 680,00 €	1 200,00 €
6.Implementácia centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov	28 923,60 €		7 680,00 €
7.Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.			4 200,00 €
8.Implementácia nástroja na centrálne riadenie ochrany pred škodlivým kódom			2 400,00 €
9.Zavedenie nástroja určeného na notifikovanie o existujúcich zraniteľnostiach programových prostriedkov a ich častí			3 000,00 €
10.Zvýšenie bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít	24 438,00 €	4 992,00 €	
11.Vypracovanie plánov kontinuíty a ich otestovanie			18 000,00 €
12.Implementácia systémov na správu a inventarizáciu aktív		76 200,00 €	

V prípade projektov kybernetickej bezpečnosti je priame vyčíslenie návratnosti pomerne komplikované. Z pohľadu návratnosti je potrebné venovať sa hodnoteniu možných škôd, ktoré by vznikli v prípade, že nebude adekvátne riešená KIB na úrovni poskytovateľa základnej služby. Ide o nasledovné potenciálne škody:

Finančné riziko – dôsledky kybernetického útoku. Ide o možné sankcie vyplývajúce priamo z legislatívnych rámcov, prípadných súdnych sporov (v prípade napríklad úniku osobných údajov) ako aj nákladov spojených so sanáciou prípadného kybernetického incidentu. Tieto finančné prostriedky nie je možné momentálne vyčísliť, reálne však môže niekoľko násobne prekročiť straty interných finančných prostriedkov univerzity.

Reputačné riziko – vzhľadom na postavenie a oblasť spoločenskej dôležitosti a zákonných povinností univerzity, je toto riziko potenciálne vysoké – teda v prípade neplnenia legislatívnych požiadaviek v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS alebo vyhlášky 362 /2018 Z. z. či reálneho výpadku prevádzky základnej služby, úniku citlivých dát v kombinácii aj s prípadnou medializáciou a pod.

9. PROJEKTOVÝ TÍM

Pre účely realizácie projektu sa zostavuje Riadiaci výbor (RV), v minimálne nasledovnom zložení:

Riadiaci výbor

- Predseda RV - prorektorka pre rozvoj prof. Bc. RNDr. Danica Kačíková, MSc., PhD.
- Vlastník procesov - vedúca odd. informačných systémov Ing. Jana Námešná
- projektový manažér - Ing. Tibor Weis - riaditeľ CIT
- zástupca dodávateľa (doplní sa po vysúťažení)

Interný projektový tím objednávateľa

- Projektový manažér - Ing. Tibor Weis - riaditeľ CIT
- IT analytik - Mgr. Svetlana Hanzélyová
- IT architekt - vedúci odd. komunikačných sietí Bc. Miroslav Ďurian
- Manažér kybernetickej a informačnej bezpečnosti - Ing. Lukáš Maťokár
- Zástupca kľúčových používateľov - vedúci odd. správy používateľov - Ing. Ján Kíšik

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Ing. Tibor Weis	riaditeľ	Centrum informačných technoloógií	Projektový manažér
2.	Mgr. Svetlana Hanzélyová	Analytik, metodik a správca IT systémov	odd. Informačných systémov	IT analytik 1
3.	Bc. Miroslav Ďurian	vedúci odd. komunikačných sietí	odd. Komunikačných sietí CIT	IT architekt
4.	Ing. Lukáš Maťokár	Analytik, metodik a správca univerzitnej siete TUZVOnet	odd. Komunikačných sietí CIT	Manažér kybernetickej a informačnej bezpečnosti
5.	Ing. Ján Kíšik	vedúci odd. Správy používateľov	odd. Správy používateľov	Kľučový používateľ
6.	Ing. Iveta Kíšiková	analytik, metodik a správca univerzitného web servera a webového redakčného systému	odd. Správy používateľov	IT analytik 2
7	Ing. Jana Námešná	analytik, metodik a správca univerzitného informačného systému	odd. Informačných systémov	vlastník procesov

Všetci členovia tímu sú internými zamestnancami TUZVO ku dňu podania ŽoNFP.

Stručne zodpovednosti jednotlivých rolí:

Projektová rola: Biznis vlastník

Zodpovedný za:

- Realizáciu dohľadu nad súladom projektových výstupov s požiadavkami koncových používateľov.
- Spoluprácu pri riešení odpovedí na otvorené otázky a riziká projektu.
- Posudzovanie, pripomienkovanie, testovanie a protokolárne odsúhlasovanie projektových výstupov v príslušnej oblasti (v biznis procese) po vecnej stránke (najmä procesnej a legislatívnej) · Riešenie problémov a požiadaviek v spolupráci s odbornými garantmi,
- Spoluprácu pri špecifikácii a poskytuje súčinnosť pri riešení zmenových požiadaviek · Schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu z pohľadu používateľov koncového produktu
- Definovanie očakávaní na kvalitu projektu, kritérií kvality projektových produktov, prínosov pre koncových používateľova požiadaviek na bezpečnosť, · Definovanie merateľných výkonnostných ukazovateľov projektov a prvkov,
- Sledovanie a odsúhlasovanie nákladovosti, efektívnosti vynakladania finančných prostriedkov a priebežné monitorovanie a kontrolu odôvodnenia projektu (BC/CBA)
- Schválenie akceptačných kritérií,
- Riešenie problémov používateľov
- Akceptáciu rozsahu a kvality dodávaných projektových výstupov pri dosiahnutí platobných míľnikov,
- Vykonanie UX a UAT testovania
- Odsúhlasenie spustenia výstupov projektu do produkčnej prevádzky,
- Dostupnosť a efektívne využitie ľudských zdrojov alokovaných na realizáciu projektu,
- Vykonávanie monitorovania a hodnotenia procesov v plánovaných intervaloch.
- Poskytovanie vyjadrení k zmenovým požiadavkám, k ich opodstatnenosti a prioritizácii
- Zisťovanie efektívneho spôsobu riadenia a optimalizácie zvereného procesu, vrátane analyzovanie všetkých vyskytujúcich sa nezhôd,
- Okrem zvažovaní rizík prevádzkových alebo podporných procesov súčasne vlastník napomáha identifikovať príležitosti,
- Zlepšovanie a optimalizáciu procesov v spolupráci s ďalšími prepojenými vlastníkmi procesov a manažérom kvality,

- Odsúhlasenie akceptačných protokolov zmenových konaní
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1 plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola: Projektový manažér objednávateľa (PM)

Zodpovedný za:

- Riadenie projektu podľa pravidiel stanovených vo Vyhláške 401/2023 Z. z.
- Riadenie prípravy, inicializácie a realizácie projektu
- Identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii ·
- Plánovanie, organizovanie, motivovanie projektového tímu a monitorovanie projektu
- Zabezpečenie efektívneho riadenia všetkých projektových zdrojov s cieľom vytvorenia a dodania obsahu a zabezpečenie naplnenie cieľov projektu
- Určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory Riadiaceho výboru (RV) pre riadenie, plánovanie a kontrolu projektu a využívanie projektových zdrojov
- Zabezpečenie vypracovania manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z. Z., Prílohou č.1
- Zabezpečenie realizácie projektu podľa štandardov definovaných vo Vyhláške 78/2020 Z.z.
- Zabezpečenie priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie v minimálnom rozsahu Vyhlášky 401/2023 Z. , Prílohy č.1
- Vypracovanie, pravidelné predkladanie a zabezpečovanie prezentácie stavov projektu, reportov, návrhov riešení problémov a odsúhlasovania manažérskej a špecializovanej dokumentácie v rozsahu určenom Vyhláškou 401/2023 Z. z., Prílohou č.1 na rokovanie RV
- Riadenie a operatívne riešenie a odstraňovanie strategických / projektových rizík a závislostí
- Predkladanie návrhov na zlepšenia na rokovanie Riadiaceho výboru (RV)
- Zabezpečenie vytvorenia a pravidelnej aktualizácie BC/CBA a priebežné zdôvodňovanie projektu a predkladanie na rokovania RV
- Celkovú alokáciu a efektívne využívanie ľudských a finančných zdrojov v projekte
- Celkový postup prác v projekte a realizuje nápravné kroky v prípade potreby
- Vypracovanie požiadaviek na zmenu (CR), návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovanie RV
- Riadenie zmeny (CR) a prípadné požadované riadenie konfigurácií a ich zmien
- Riadenie implementačných a prevádzkových aktivít v rámci projektov.
- Aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov,
- Formálnu administráciu projektu, riadenie centrálneho projektového úložiska, správu a archiváciu projektovej dokumentácie
- Kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom,
- Dodržiavanie metodík projektového riadenia,
- Predkladanie požiadaviek dodávateľa na rokovanie Riadiaceho výboru (RV),Vecnú a procesnú administráciu zúčtovania dodávateľských faktúr

Projektová rola: KĽUČOVÝ POUŽIVATEĽ (end user)

Zodpovedný za:

- Návrh a špecifikáciu funkčných a technických požiadaviek
- Jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy) z pohľadu vecno-procesného a legislatívy
- Vytvorenie špecifikácie, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, · Špecifikáciu požiadaviek koncových používateľov na prínos systému
- Špecifikáciu požiadaviek na bezpečnosť,
- Návrh a definovanie akceptačných kritérií,
- Vykonanie používateľského testovania funkčného používateľského rozhrania (UX testovania)
- Finálne odsúhlasenie používateľského rozhrania
- Vykonanie akceptačného testovania (UAT)
- Finálne odsúhlasenie a akceptáciu manažérskych a špecializovaných produktov alebo projektových výstupov
- Finálny návrh na spustenie do produkčnej prevádzky,
- Predkladanie požiadaviek na zmenu funkcionalít produktov
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
- Realizáciu kvalitatívneho používateľského výskumu (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie rozhovoru a vyhodnotenie výskumu).
- Realizáciu kvantitatívneho používateľského výskumu (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie dotazníku a vyhodnotenie výskumu).
- Syntetizáciu biznis, technických a používateľských požiadaviek.
- Realizáciu formatívnych a sumatívnych testovaní použiteľnosti (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie rozhovoru a vyhodnotenie výskumu).
- Návrh informačnej architektúry a to najmä metódami triedenia kariet (card sorting), návrhom mapy stránky a screen flow.
- Tvorbu, testovanie a iteráciu prototypov – napr. pomocou Axure, Sketch, Figma alebo Adobe XD
- Mapovanie zákazníckych ciest

- Analýzu a návrh riešenia problematiky prístupnosti webových sídiel,
- Podporu a spoluprácu pri tvorbe Stratégie riadenia kvality (princípy, kritériá kvality),
- Spoluprácu pri vytváraní funkčných požiadaviek na výstupy z pohľadu dohľadu a UX,
- Vedenie a aktualizáciu príslušných projektových výstupov a registrov,
- Hodnotenie jednotlivých verzií výstupov projektu z pohľadu dohľadu, kontroly a UX v jednotlivých etapách,
- Vytváranie hodnotiacich kritérií na dohľad výstupov a príslušných záznamov, o ktorých reportuje projektovému manažérovi objednávateľa,
- Nastavenie a dohľad nad procesom testovania a pripomienkovanie stratégie testovania, plánov a testovacích scenárov,
- Účasť na kontrolných aktivitách počas implementácie výstupov
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

-

Projektová rola: IT analytik

Zodpovedný za:

- Vykonanie analýzy procesných a ďalších požiadaviek a vytvorenie špecifikácie súčasného alebo budúceho užívateľa softwaru („zákazníka“) a následne navrhuje dizajn a programátorské riešenie.
- Participáciu na vývoji nových, ale i vylepšovaní existujúcich aplikácií v rámci celého vývojového cyklu – systémová analýza, dizajn, kódovanie, užívateľské testovanie, implementácia, podpora, dokumentácia. Úzko spolupracuje aj s IT architektom.
- Analýza potrieb zákazníka vrátane tvorby úplnej analytickej dokumentácie a vstupov do verejného obstarávania (VO).
- Mapovanie požiadaviek do návrhu funkčných riešení.
- Návrh a správa katalóg požiadaviek - registra požiadaviek riešenia
- Analýza funkčných a nefunkčných požiadaviek,
- Návrh fyzického a logického modelu,
- Návrh testovacích scenárov,
- V priebehu implementácie robí dohľad nad zhodou výstupov s pôvodným analytickým zadaním.
- Zodpovednosť za dodržovanie správnej metodiky pri postupe analýzy
- Definovanie akceptačných kritérií v projekte
- Odsúhlasenie opisu produktov, ktoré predstavujú vstupy alebo výstupy (priebežné alebo konečné) úloh dodávateľov, alebo ktoré ich priamo ovplyvňujú a zabezpečovať akceptáciu produktov po ich dokončení
- Priraďuje priority a poskytuje stanoviská používateľov na rozhodnutia Riadiaceho výboru projektu – k realizácii zmenových požiadaviek
- Poskytuje merania aktuálneho stavu pre potreby porovnania s výsledkami projektu vzhľadom na realizáciu prínosov
- Rieši požiadavky používateľov a konflikty iných priorít
- Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

-

Projektová rola: IT architekt

Zodpovedný za:

- Navrhovanie architektúry IT riešení s cieľom dosiahnuť najlepšiu efektivitu.
- Transformovanie cieľov, prísľubov a zámerov projektu do tvorby reálnych návrhov a riešení.
- Navrhovanie takých riešení, aby poskytovali čo najvyššiu funkčnosť a flexibilitu. ·
- Posudzovanie vhodnosti navrhnutých riešení s ohľadom na požiadavky projektu. ·
- Zodpovednosť za technické navrhnutie a realizáciu projektu.
- Zodpovednosť za vytvorenie technickej IT dokumentácie a jej následná kontrola. ·
- Zodpovednosť za definovanie integračných vzorov, menných konvencií, spôsobov návrhu a spôsobu programovania.
- Definovanie architektúry systému, technických požiadaviek a funkčného modelu (Proof Of Concept.)
- Vytvorenie požiadaviek na HW/SW infraštruktúru IS
- Udržiavanie a rozvoj konzistentnej architektúry s dôrazom na architektúru aplikačnú, dátovú a infraštruktúru
- Analýzu a odhad náročnosti technických požiadaviek na vytvorenie IS alebo vykonanie zmien v IS
- Navrhovanie riešení zohľadňujúce architektonické štandardy, časové a zdrojové obmedzenia,
- Navrhovanie dátových transformácií medzi dátovými skladmi a aplikáciami
- Vyhodnocovanie implementačných alternatív z pohľadu celkovej IT architektúry
- Ladenie dátových štruktúr za účelom dosiahnutia optimálneho výkonu
- Prípravu akceptačných kritérií · Analýza nových nástrojov, produktov a technológií
- Správa, rozvoj a dohľad nad dodržiavaním integračných štandardov
- Priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane Detailného návrhu riešenia (DNR) z pohľadu analýzy a návrhu riešenia architektúry IS
- Vykonáva posudzovanie a úpravu testovacej stratégie, testovacích scenárov, plánov testov, samotné testovanie a účasť na viacerých druhoch testovania

- Vykonanie záťažových, výkonnostných a integračných testov a navrhnutie následných nápravných
- Nasadenie a otestovanie migrácie, overenie kvality dát a navrhnutie nápravných opatrení
- Participáciu na výkone bezpečnostných testov,
- Participáciu na výkone UAT testov,
- Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola: manažér kybernetickej a informačnej bezpečnosti

Zodpovedný za:

- špecifikovanie štandardov, princípov a stratégií v oblasti ITB a KIB,
- ak je projekt primárne zameraný na problematiku ITB a KIB – je priamo zodpovedný za špecifikáciu a analýzu funkčných požiadaviek na ITB a KIB,
- špecifikovanie požiadaviek na ITB a KIB, kontroluje ich implementáciu v realizovanom projekte,
- špecifikovanie požiadaviek na bezpečnosť vývojového, testovacieho a produkčného prostredia,
- špecifikovanie funkčných a nefunkčných požiadaviek pre oblasť ITB a KIB,
- špecifikovanie požiadaviek na bezpečnosť v rámci bezpečnostnej vrstvy,
- špecifikovanie požiadaviek na školenia pre oblasť ITB a KIB,
- špecifikovanie požiadaviek na bezpečnostnú architektúru riešenia a technickú infraštruktúru pre oblasť ITB a KIB,
- špecifikovanie požiadaviek na dostupnosť, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na ITB a KIB,
- realizáciu posúdenie požiadaviek agendy ITB a KIB na integrácie a procesov konverzie a migrácie, identifikácia nesúladu a návrh riešenia
- špecifikovanie požiadaviek na ITB a KIB, bezpečnostný projekt a riadenie prístupu,
- špecifikovanie požiadaviek na testovanie z hľadiska ITB a KIB, realizáciu kontroly zapracovania a retestu,
- špecifikovanie požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť ITB a KIB, ako aj v zmysle "best practies",
- špecifikovanie požiadaviek na dodanie potrebnej dokumentácie súvisiacej s ITB a KIB kontroluje ich implementáciu v realizovanom projekte,
- špecifikovanie požiadaviek a konzultácie pri návrhu riešenia za agendu ITB a KIB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný návrh riešenia (DNR)“,
- špecifikáciu požiadaviek na bezpečnosť IT a KIB v rámci procesu "akceptácie, odovzdania a správy zdroj. kódov“
- špecifikáciu akceptačných kritérií za oblasť ITB a KIB,
- špecifikáciu pravidiel pre publicitu a informovanosť s ohľadom na ITB a KIB,
- poskytovanie konzultácií pri tvorbe šablón a vzorov dokumentácie pre oblasť ITB a KIB,
- získavanie informácií nutných pre plnenie úloh v oblasti ITB a KIB,
- špecifikáciu podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť ITB a KIB,
- konzultácie a vykonávanie kontrolnej činnosť zameranej na obsah a komplexnosť dok. z hľadiska ITB a KIB,
- špecifikáciu požiadaviek na bezpečnostný projekt pre oblasť ITB a KIB,
- realizáciu kontroly zameranej na naplnenie požiadaviek definovaných v bezp. projekte za oblasť ITB a KIB
- realizáciu kontroly zameranú na správnosť nastavení a konfigurácii bezpečnosti jednotlivých prostredí,
- realizáciu kontroly zameranú realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť a kompletný popis rozhraní, správnu identifikácia závislostí,
- realizáciu kontroly naplnenia definovaných požiadaviek pre oblasť ITB a KIB,
- realizáciu kontroly zameranú na implementovaný proces v priamom súvise s ITB a KIB,
- realizáciu kontroly súladu s planou legislatívou v oblasti ITB a KIB (obsahuje aj kontrolu leg. požiadaviek)
- realizáciu kontroly zameranú zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní a spoločných komponentov a posúdenia z pohľadu bezpečnosti, · poskytovanie konzultácií a súčinnosti pre problematiku ITB a KIB,
- získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti ITB a KIB,
- aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1 plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

10. PRÍLOHY

Príloha : 1 Zoznam rizík a závislostí