PRÍSTUP K PROJEKTU

Vzor pre manažérsky výstup I-03

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

Povinná osoba	*Slovenský hydrometeorologický ústav*
Názov projektu	*Rozvoj kybernetickej a informačnej bezpečnosti v SHMÚ*
Zodpovedná osoba za projekt	*RNDr. Ondrej Tóth*
Realizátor projektu	*Slovenský hydrometeorologický ústav*
Vlastník projektu	*Slovenský hydrometeorologický ústav*

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	RNDr. Ondrej Tóth	SHMÚ	Manažér IB	13.6.2024	

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
0.1	*10.6.2024*	*Pracovný návrh*	OTO
1.0	*13.6.2024*	*Verzia k ŽoNFP*	OTO

2. ÚČEL DOKUMENTU

V súlade s Vyhláškou 401/2023 Z.z. je dokument I-03 Prístup k projektu určený na rozpracovanie detailných informácií prípravy projektu z pohľadu aktuálneho stavu, budúceho stavu a navrhovaného riešenia.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	**POPIS**
AR	Analýza rizík
IS	Informačný systém
ITVS	Informačné technológie verejnej správy
KIB	Kybernetická a informačná bezpečnosť
METAIS	Centrálny metainformačný systém verejnej správy
SHMÚ	Slovenský hydrometeorologický ústav
VO	Verejné obstarávanie
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
ZoITVS	Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

2.2 Konvencie pre typy požiadaviek (príklady)

Požiadavky majú nasledovnú konvenciu:

FWxx – požiadavky týkajúce sa bezpečnostného riešenia perimetra siete (firewall)

- xx – číslo požiadavky

BPxx – požiadavky týkajúce sa bezpečnostného riešenia pre oblasť zálohovania

- xx – číslo požiadavky

3. POPIS NAVRHOVANÉHO RIEŠENIA

SHMÚ monitoruje kvantitatívne a kvalitatívne parametre stavu ovzdušia a vôd na území Slovenskej republiky, zhromažďuje, overuje, hodnotí, archivuje a interpretuje údaje a informácie o stave a režime ovzdušia a vôd, popisuje deje v atmosfére a hydrosfére, tvorí a vydáva meteorologické a hydrologické predpovede, výstrahy a informácie. Údaje, informácie a výsledky štúdií poskytuje užívateľom a verejnosti. Najmä v oblasti vydávania predpovedí, výstrah pred nebezpečnými meteorologickými a hydrologickými javmi sa SHMÚ v spolupráci s orgánmi krízového riadenia podieľa na prevencii pre negatívnymi dopadmi na spoločnosť a zmenšovaní potenciálnych materiálnych škôd.

Cieľom projektu je zaistenie kybernetickej ochrany v podmienkach SHMÚ v súlade so zákonom ZoKB a ZoITVS vo vybraných oblastiach. Projekt adresuje dve oblasti, kde vykonaná analýza rizík identifikovala najzávažnejšie nedostatky v bezpečnostných opatreniach. Tieto nedostatky boli konštatované aj nezhodami z auditov a odporúčaniami audítora. Jedná sa o oblasť sieťovej bezpečnosti (bezpečnostné riešenie segmentu perimetra siete - firewall) a oblasti prevádzky informačných systémov a biznis kontinuity (zálohovanie). Obsahom projektu v oboch oblastiach je obstaranie bezpečnostného riešenia pozostávajúceho z HW komponentov, licencií, implementačných a podporných služieb. Ich konkrétna skladba je uvedená v kapitole technologickej vrstvy.

Projekt zabezpečuje podporu v oblasti informatizácie a digitálnej transformácie (Kybernetická a informačná bezpečnosť) v oblastiach:
- posilnenie prvkov kritickej infraštruktúry a budovanie nástroja pre manažment údajov;
- podpora včasnej detekcie a zvýšenie schopnosti reakcie na kybernetické bezpečnostné incidenty a na adaptácia najmodernejších technológií, na zvýšenie odolnosti základných služieb pred kybernetickými hrozbami, vrátane podpory inovatívnych produktov a služieb

SHMÚ má dostatočné administratívne a prevádzkové kapacity na realizáciu projektu a zabezpečenie udržateľnosti.

4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

4.1 Biznis vrstva

SHMÚ je v zmysle ZoKB prevádzkovateľom základnej služby. Zaradenie informačných systémov základnej služby v prostredí SHMÚ do kategórií v zmysle ZoKB:
kategória I – 2 ks informačných systémov
kategória II – 7 ks informačných systémov
Počet prvkov kritickej infraštruktúry – 4ks

V rámci auditu kybernetickej bezpečnosti bola konštatovaná súčasná implementácia bezpečnostných opatrení na 61% v súlade so zákonnými požiadavkami. Po ukončení projektu je plánované zabezpečenie súladu na 70-80%.

4.2 Aplikačná vrstva

Aktuálne informácie o službách a informačných systémoch v SHMÚ, na ktoré má závažný bezpečnostný incident dopad, sú evidované v METAIS (v prevádzke alebo plánované naďalej používať a rozvíjať):

Kód MetaIS	Názov
isvs_10889	Evidenčný a notifikačný systém oprávnených meraní a technických činností
isvs_11047	IS SK BIO
isvs_11085	Zverejňovanie informácií na webovom sídle: https://oeab.shmu.sk/
isvs_308	Informačný systém Hydrologická informačná a predpovedná služba
isvs_309	Klimatologický a Meteorologický informačný Systém
isvs_310	Súhrnná evidencia o vodách
isvs_311	Čiastkový monitorovací systém "Rádioaktivita životného prostredia"
isvs_312	Informačný systém Kvalita ovzdušia
isvs_329	Národný register znečisťovania z oblasti vody, ovzdušia, odpadov a pôdy
isvs_7297	Mzdový a personálny systém SHMÚ Magma HCM
isvs_7298	Dochádzkový systém SHMÚ ID.EST Sense
isvs_7299	Ekonomický systém SHMÚ SOFTIP
isvs_7300	Registratúrny systém SHMÚ Nuntio
isvs_9523	Optimalizácia dátových tokov v oblasti kvantity a kvality vody
isvs_9525	Národný Emisný Informačný Systém
isvs_9526	Hydrologický informačný systém
isvs_9527	ZBERNÉ INFORMAČNÉ SYSTÉMY SHMÚ
isvs_9528	IS HYPOS – POVAPSYS
isvs_9649	Informačný systém pre operatívnu meteorológiu

Cieľom projektu je aplikovať opatrenia v lokálnej infraštruktúre SHMÚ. Potenciálny incident na prvku perimetra siete však môže znamenať dopad na všetky vymenované služby a systémy.

4.3 Dátová vrstva

N/A

4.4 Technologická vrstva

Oblasť bezpečnostného riešenia perimetra siete (firewall)

Bezpečnostné riešenie perimetra siete obsahuje prvky nesúce funkcionality NGFW (next generation firewall), centrálnleho prepínača (core switch) a VPN brány (VPN gateway).

Oblasť bezpečnostného riešenia pre zálohovanie

Bezpečnostné riešenie zálohovania obsahuje prvky nesúce funkcionality páskovej knižnice – alebo ekvivalentného riešenia, modulu na zabezpečenie kopírovania údajov cez WAN a rozšírenie existujúceho zálohovacieho SW Veeam o potrebné licencie.

4.4.1 Prehľad technologického stavu - AS IS

Oblasť bezpečnosť siete:

Perimeter siete v súčasnosti zabezpečujú komponenty inštalované v roku 2015 (firewall, VPN gateway, core switche). Zariadenia sú po životnosti bez možnosti ďalších bezpečnostných aktualizácií, takže sa prevádzkujú s niektorými neošetrenými zraniteľnosťami. SHMÚ nemá prístup ku všetkým komponentom manažmentu (vendor lock-in). Jedným z dôsledkov je aj to, že sa v dôsledku periodického zahltenia musí firewall proaktívne reštartovať dvakrát týždenne, čo má dopad (v rôznom rozsahu pre každé) na všetky

existujúce spojenia v danej chvíli. VPN gateway neumožňuje efektívnym spôsobom nasadiť dvojfaktorovú autentifikáciu pre vzdialený prístup. Z dôvodu morálnej zastaranosti komponentov sa nedajú efektívne implementovať moderné prístupy pre zabezpečenie sieťovej prevádzky. Existujúce riešenie tiež obmedzuje do budúcnosti pokryť zvyšujúce sa nároky na priepustnosť siete.

Oblasť zálohovanie:

SHMÚ vykonáva zálohovanie podľa aktuálneho zálohovacieho plánu s použitím systému od výrobcu Veeam. Zálohy sa ukladajú na úložisko, ktoré je v tej istej budove asi 15 m od samotného dátového centra, čo je z hľadiska biznis kontinuity vyhodnotené ako riziko. V minulosti sa na mitigáciu tohto rizika vybrané zálohy kopírovali na záložnú lokalitu - prevádzkovanú NASES-om v Devínskej Novej Vsi v rámci Memoranda o spolupráci. Úložné kapacity na záložnej lokalite sú však v dôsledku riešenia rôznych havarijných stavov v poruchovom stave a kopírovanie záloh na vzdialenú lokalitu sa momentálne nevykonáva.

4.4.2 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Pozri katalóg požiadaviek.

4.5 Bezpečnostná architektúra

N/A

5. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

N/A

6. ZDROJOVÉ KÓDY

N/A

7. PREVÁDZKA A ÚDRŽBA

Oblasť bezpečnostného riešenia perimetra siete (firewall)

Do požiadaviek bola zahrnutá v súlade s podmienkami projektu podpora bezpečnostného riešenia na jeden rok.

Oblasť bezpečnostného riešenia pre zálohovanie

Do požiadaviek bola zahrnutá v súlade s podmienkami projektu podpora Veeam riešenia na jeden rok.

8. POŽIADAVKY NA PERSONÁL

Zostavuje sa Riadiaci výbor (RV), v minimálnom zložení:

- Predseda RV
- Biznis vlastník
- Konečný používateľ
- Zástupca dodávateľa (bez hlasovacieho práva)

Zostavuje sa Projektový tím

- Projektový manažér
- Manažér kybernetickej a informačnej bezpečnosti
- Vecne príslušný odborný garant (prevádzka, infraštruktúra)
- Expert dodávateľa (podľa jednotlivých oblastí a aktivít)

ID	Meno a Priezvisko	Pozícia	Oddelenie/úsek	Rola v projekte

1.	RNDr. Ondrej Tóth	Poverený riaditeľ úseku informatika	Informačné technológie	Manažér informačnej a kybernetickej bezpečnosti
2.	Ing. Martin Borecký	Vedúci odboru IT	Informačné technológie	Vecný garant
4.	Zatiaľ neobsadené	Projektové riadenie	Odbor prípravy a implementácie projektu	Projektový manažér
5.	Zatiaľ neobsadené	Zástupca dodávateľa	Dodávateľ	Expert dodávateľa

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Implementácia bezpečnostných riešení (v katalógu požiadaviek označených ako Inkrement 1 a Inkrement 2) pre jednotlivé oblasti je vzájomne nezávislá. Obe riešenia budú implementované dodávateľským spôsobom – dodávateľ nasadí riešenie v prostredí objednávateľa. Obe strany budú súčinné tak, aby nasadenie prebehlo podľa možnosti bezvýpadkovým spôsobom.

10. PRÍLOHY

Katalóg požiadaviek