IDEOVÝ ZÁMER

Podpora v oblasti kybernetickej a informačnej bezpečnosti v Štátnom geologickom ústave Dionýza Štúra

Identifikácia projektu

Názov:	Podpora v oblasti kybernetickej a informačnej bezpečnosti v Štátnom geologickom ústave Dionýza Štúra
Realizátor:	Štátny geologický ústav Dionýza Štúra
Kontaktná osoba:	PhDr. Vladimíra Pazderová, PhD. Karol Fazekaš
Dátum:	27.6.2024
Predpokladaný začiatok:	01.01.2025
Dátum schválenia projektovou komisiou:	

1. POPIS PROJEKTU

1.1. STRUČNÝ POPIS VÝCHODISKOVEJ SITUÁCIE

Štátny geologický ústav Dionýza Štúra, ktorý je v zmysle zákona č. 69/2018 Z. z. poskytovateľom základnej služby, stojí v súčasnosti podobne ako ďalšie orgány verejnej správy pred výzvami v oblasti kybernetickej a informačnej bezpečnosti (ďalej len "KIB"), ktoré vyplývajú z rýchleho rozvoja digitálnych technológií a neustáleho zvyšovania množstva citlivých dát, ktoré je potrebné ochraňovať. Zvyšujú sa teda hrozby, zraniteľnosti a následne aj dopady bezpečnostných incidentov. V zmysle platnej legislatívy nastavujú požiadavky a štandard z pohľadu KIB práve zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe.

Štátny geologický ústav je prevádzkovateľom nasledovnej základnej služby:

- Správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

Na prevádzke danej základnej služby sa podieľajú tieto systémy:

- Podnikový informačný systém Štátneho geologického ústavu D. Štúra
- Digitálny archív
- Geologický informačný systém

Štátny geologický ústav má relatívne rozsiahlu infraštruktúru informačných systémov a aplikácií, prostredníctvom ktorých poskytuje služby verejnosti.

Úroveň služieb všetkých dotknutých subjektov priamo závisí od funkčnosti informačných systémov organizácie a niektoré služby sú od ich schopnosti prevádzky dokonca plne závislé. Nedostupnosť informačných aktív v dôsledku kybernetického incidentu preto môže mať fatálny vplyv nielen na základnú službu a poskytovanie ostatných služieb ústavu ale i organizácií, ktoré sú na jeho infraštruktúru naviazané.

Z dôvodu zabezpečenia súladu s požiadavkami zákonov o kybernetickej bezpečnosti a informačných technológiách vo verejnej správe bolo externým dodávateľ vykonaný audit kybernetickej bezpečnosti. Audit odhalil viaceré kritické oblasti, ktoré bezprostredne alebo potenciálne ohrozujú poskytovanie základnej služby. Časť opatrení eliminujúcich bezpečnostné riziká súvisiace s prevádzkou informačných systémov bola vykonaná. Vzhľadom na obmedzené zdroje (finančné, personálne) ale neboli realizované všetky potrebné opatrenia, a preto je nevyhnutné realizovať ďalšie opatrenia, ktoré umožnia ďalšie zvýšenie bezpečnosti ich prevádzky. S ohľadom na uvedené sa ako najvýznamnejšie problémy čoraz viac prejavujú:

1. **Nedostatočné riadenie rizík a zraniteľností:** Štátny geologický ústav čelí bez jasného prehľadu o tom, kde presne je zraniteľný, riziku neefektívneho využívania zdrojov na ochranu aktív alebo k opomenutiu kritických hrozieb. V oblasti riadenia rizík chýba nástroj, ktorý by efektívne preskúmaval a aktualizoval identifikované riziká v závislosti od prijatých bezpečnostných opatrení.
2. **Neúplná alebo neaktualizovaná bezpečnostná a riadiaca dokumentácia:** Absencia alebo zastaranie interných smerníc a postupov v oblasti kybernetickej bezpečnosti môže viesť k nesúladu s aktuálnymi legislatívnymi požiadavkami ako aj aktuálnym bezpečnostným stavom.
3. **Problémy s kontinuitou činností pri krízových situáciách:** V prípade krízovej situácie ako kybernetického bezpečnostného útoku alebo vzniknutého incidentu neexistujú postupy pre obnovu napadnutých systémov. Nedostatočná príprava na tieto udalosti môže viesť k dlhodobému prerušeniu služieb a ťažko obnoviteľným finančným a operačným škodám.
4. **Nedostatočné monitorovanie a detekcia hrozieb v reálnom čase:** Absencia komplexných systémov pre monitorovanie a reakciu na bezpečnostné incidenty v reálnom čase obmedzuje schopnosť efektívne reagovať na potenciálne hrozby.
5. **Nedostatočné riadenie prístupov k aplikáciám a údajom:** Nedostatočná kontrola a správa prístupových práv môže viesť k neoprávnenému prístupu, čo zvyšuje riziko zneužitia informácií a potenciálnych bezpečnostných incidentov. Absencia centralizovaného a automatizovaného systému na správu prístupových práv sťažuje identifikáciu, monitorovanie a riadenie prístupov zamestnancov a externých partnerov.
6. **Nedostatočná správa a aktualizácia softvérových záplat (patch) a endpointov:** Nedostatok efektívneho nástroja na patch a endpoint manažment môže viesť k zraniteľnostiam v systémoch, ktoré útočníci môžu zneužiť. Tento problém zahŕňa oneskorené alebo neúplné nasadzovanie aktualizácií, čo môže mať za následok zvýšené riziko kybernetických útokov a nespoľahlivosť IT infraštruktúry.

7. **Zastaraná a nehomogénna sieťová infraštruktúra:** Štátny geologický ústav má staré a rôzne sieťové prvky, ktoré potrebujú výmenu a modernizáciu, vrátane zabezpečenia redundancie a zlepšenia sieťovej segmentácie.
8. **Zraniteľná serverová infraštruktúra:** Používanie zariadení, ktoré sú na konci svojej životnosti (EOL - End of Life), predstavuje bezpečnostné riziko a môže ohroziť dostupnosť poskytovaných služieb.
9. **Nedostatočná validácia efektivity zavedených bezpečnostných opatrení:** Potreba vykonať audit a penetračné testy na konci projektu s cieľom validovať účinnosť implementovaných bezpečnostných opatrení a identifikovať zostávajúce potrebné oblasti zlepšenia.

Práve s ohľadom na vyššie uvedené nedostatky je predmetom projektu súbor riešení, ktoré zlepšia celkovú úroveň kybernetickej bezpečnosti organizácie a umožnia dosiahnuť požadovanú úroveň jeho KIB v súlade s platnou legislatívou.

Zámerom projektu je posilniť kybernetickú a informačnú bezpečnosť Štátneho geologického ústavu prostredníctvom komplexného prístupu zameraného na zlepšenie viditeľnosti a kontroly nad informačnou infraštruktúrou. V rámci projektu sa budú realizovať nasledujúce kľúčové opatrenia:

1. **Aktualizácia analýzy rizík a implementácia integrovaného informačného systému pre identifikáciu a riadenie rizík,** ktorý zahŕňa funkcionalitu správy aktív, zraniteľností, hrozieb a opatrení. Systém umožní dynamické aktualizovanie a hodnotenie rizík založené na aktuálnych dátach a poskytne nástroje pre efektívne riadenie a minimalizáciu rizík.
2. **Vypracovanie, aktualizácia a implementácia smerníc a plánov pre rozvoj IT vyplývajúcich z aktuálnej legislatívy týkajúcej sa KIB -** Prísne dodržiavanie aktuálnej legislatívy a bezpečnostných štandardov prostredníctvom implementácie a aktualizácie relevantných smerníc zníži zraniteľnosti vyplývajúce z nedostatočného riadenia a dodržiavania opatrení kybernetickej bezpečnosti.
3. **Vypracovanie a implementácia komplexného plánu kontinuity činností (BCM),** ktorý zahŕňa postupy pre rýchlu obnovu kritických systémov a služieb po narušení. Plán bude obsahovať scenáre pre rôzne typy udalostí a zahrnie analýzu funkčných dopadov, strategické zdroje na obnovu a časové rámce pre reakciu.
4. **Zavedenie systému pre riadenie prístupov IDM** umožní efektívne prideľovanie, monitorovanie a revíziu prístupových práv, čím sa zabezpečí, že k citlivým údajom a aplikáciám budú mať prístup len oprávnené osoby. Zavedenie IDM systému poskytne centralizovanú platformu pre správu prístupov, zjednoduší auditovanie a zvýši celkovú bezpečnosť IT infraštruktúry.
5. **Zavedenie systému pre správu a aktualizáciu softvérových záplat a endpointov:** Implementácia nástroja na správu záplat a endpointov zabezpečí, že všetky systémy budú pravidelne a včas aktualizované, čím sa zlepší celková bezpečnosť a výkon IT prostredia.
6. **Modernizácia sieťovej infraštruktúry v informačnej sieti:** Zabezpečí sa výmena zastaraných sieťových prvkov, dobudovanie záložných trás a rozšírená segmentácia siete. Tieto kroky významne prispejú k zníženiu zraniteľností vyplývajúcich z používania EOL zariadení a ich nedostatočného zabezpečenia.
7. **Modernizácia serverovej infraštruktúry:** Výmena serverových komponentov, sieťových prvkov prispeje k zníženiu rizika nízkej dostupnosti poskytovania základnej služby a zraniteľnosti spojenej s používaním zastaraných zariadení.
8. **Vykonanie auditu kybernetickej bezpečnosti:** Vykonanie auditov a penetračných testov na konci projektu poskytne hodnotné prehľady o efektívnosti prijatých opatrení a pomôže identifikovať ďalšie možnosti zlepšenia.

Implementáciou týchto technických opatrení v rámci celkového projektu zabezpečenia, že v oblasti kybernetickej a informačnej bezpečnosti sa zvýši odolnosť ústavu proti kybernetickým hrozbám a zlepší sa ochrana dát a základnej služby.

Zvyšovanie úrovne v oblastiach procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia je nevyhnutné pre zvýšenie kapacít organizácie v oblasti kybernetickej a informačnej bezpečnosti. To zahŕňa nielen aktualizáciu a posilnenie fyzickej a IT infraštruktúry, ale aj budovanie a rozvoj organizácie KIB, aby bola organizácia schopná plniť úlohy v tejto oblasti.

Cieľová skupina tohto projektu zahŕňa nielen zamestnancov štátneho geologického ústavu, ale aj občanov, ktorí sa spoliehajú na digitálne služby poskytované ústavom.

Projekt si tiež kladie za cieľ podporiť včasnú detekciu kybernetických incidentov a zvýšiť schopnosť reakcie organizácie na takéto hrozby. Je dôležité adaptovať najmodernejšie technológie a postupy, čím sa zvýši odolnosť základnej služby organizácie proti kybernetickým hrozbám.

Vzhľadom na komplexnosť a dôležitosť tohto projektu je prioritou jeho včasná realizácia, aby sa predišlo potenciálnym rizikám a zabezpečila vysoká úroveň ochrany pre všetky zainteresované strany.

Realizácia vyššie navrhovaných opatrení umožní vytvoriť robustnejšiu infraštruktúru, ktorá bude funkčne a kapacitne vyhovovať potrebám nevyhnutným pre poskytovanie služieb organizácie a z bezpečnostného hľadiska spĺňať legislatívne požiadavky. Zároveň umožní nastaviť procesy a postupy, ako tento stav v čase zachovať a rozvíjať v nadväznosti na požiadavky vyplývajúce zo zmeny legislatívy resp. rozsahu poskytovaných služieb.

1.2. SITUÁCIA PO REALIZÁCII PROJEKTU

Po úspešnej implementácii projektu sa predpokladá výrazné posilnenie kybernetickej a informačnej bezpečnosti. Tento projekt prináša komplexné vylepšenia v rôznych oblastiach, zaručujúc robustnejšiu ochranu pre infraštruktúru organizácie a zvyšujúc odolnosť proti kybernetickým hrozbám.

V oblasti infraštruktúry dôjde k výraznému posilneniu prostredníctvom zavedenia pokročilých monitorovacích a reakčných systémov. Tieto opatrenia zabezpečia rýchlejšie odhaľovanie a reagovanie na bezpečnostné incidenty, čo je kľúčové pre minimalizáciu rizík a potenciálnych škôd.

Modernizácia serverovej a zálohovacej infraštruktúry posilní schopnosť štátneho geologického ústavu udržať nepretržitú dostupnosť kritických služieb a efektívne reagovať na incidenty súvisiace so stratou údajov.

Implementácia a aktualizácia smerníc a plánov pre rozvoj IT prispejú k zabezpečeniu súladu s legislatívnymi požiadavkami a najnovšími štandardmi v oblasti kybernetickej bezpečnosti.

Výsledkom realizácie projektu bude organizácia, ktorá je nielen lepšie chránená pred kybernetickými hrozbami, ale je tiež pripravená na využívanie digitálnych príležitostí s väčšou dôverou a bezpečnosťou pre všetkých užívateľov.

1.3. ÚPRAVA PROCESOV

Vychádzajúc z výsledkov auditu kybernetickej bezpečnosti, ktorý odhalil potrebné oblasti zlepšenia, sa organizácia zameria na predbežné úpravy svojich procesov pred zavedením vybraných opatrení.

Prvým krokom bude dôkladná analýza a optimalizácia súčasných procesov, aby sa zabezpečilo, že nové technológie budú implementované efektívne a budú podporovať už existujúce zjednodušené postupy. Týmto sa zvýši celková úroveň kybernetickej a informačnej bezpečnosti v ústave.

Následne sa zameria na integráciu nových opatrení tak, aby sa prirodzene integrovali do upravených procesov. To bude zahŕňať aktualizáciu interných smerníc a príslušnej dokumentácie, čím sa zabezpečí súlad s novými postupmi a technológiami. Tento prístup umožní hladkú integráciu a zvýši efektivitu nových riešení v rámci organizácie. Kľúčovou súčasťou bude aj zaškolenie zamestnancov, ktoré im poskytne potrebné znalosti a zručnosti pre prácu s novými nástrojmi a v rámci optimalizovaných procesov. To zvýši ich schopnosť efektívne reagovať na bezpečnostné výzvy a prispieť k ochrane identifikovaných aktív organizácie. Celkovo, po implementácii týchto opatrení, bude ústav lepšie vybavený na detekciu a reakciu na kybernetické hrozby, čo výrazne zvýši úroveň KIB. Zvýšená kybernetická a informačná odolnosť tak prispeje k posilnenej dôvere v digitálne služby, ktoré štátny geologický ústav poskytuje.

2. POUŽÍVATELIA RIEŠENIA

Počas vykonaného auditu kybernetickej bezpečnosti sa aktívne získavali názory kľúčových používateľov, ktoré poskytli detailný pohľad do súčasného stavu a identifikovali kritické oblasti potrebné pre zlepšenie. Tento proces odhalil, že používatelia vnímajú problémy súvisiace s ochranou dát, prístupnosťou k systémom a celkovou pripravenosťou na kybernetické hrozby. Aj na základe týchto informácií sa navrhli zlepšenia, ktoré boli výsledkom realizovaného auditu.

V rámci projektu budú kľúčoví používatelia zapojení do fázy implementácie a testovania opatrení, aby sa zabezpečilo, že konečné výsledky budú reflektovať ich potreby a zlepšia celkovú kybernetickú a informačnú bezpečnosť. Okrem toho bude zabezpečené, že všetci používatelia budú adekvátne oboznámení a zaškolení na prácu s novými systémami a procesmi, čo zvýši ich efektivitu a prispeje k bezpečnejšiemu prostrediu ústavu.

Týmto spôsobom sa organizácia zaväzuje k tomu, že vývoj a implementácia nových bezpečnostných opatrení budú v súlade s potrebami a očakávaniami tých, ktorí ich budú najviac využívať, čo prispieva k vyššej úrovni spokojnosti a bezpečnosti pre všetkých.

3. PRÍNOSY

V rámci projektu zameraného na zvýšenie kybernetickej a informačnej bezpečnosti v organizácii sme identifikovali nasledovné prínosy, ktoré prinesie realizácia tohto projektu. Tieto prínosy sú spojené s konkrétnymi problémovými oblasťami, ktoré identifikoval realizovaný audit kybernetickej bezpečnosti.

1) **Zvýšenie úrovne kybernetickej a informačnej bezpečnosti -** Implementáciou opatrení v rámci projektu očakávame zníženie počtu identifikovaných kritických rizík aj na základe výsledkov vykonaného auditu a analýzy rizík na konci projektu.
2) **Zníženie počtu bezpečnostných incidentov:** Vďaka posilnenej kybernetickej a informačnej bezpečnosti očakávame pokles počtu bezpečnostných incidentov v organizácii.
3) **Zlepšená spokojnosť a dôvera používateľov:** Implementácia projektu by mala viesť k vyššej spokojnosti používateľov a zamestnancov s digitálnymi službami, čo zvýši ich dôveru v tieto služby.
4) **Posilnené povedomie o kybernetickej bezpečnosti:** V rámci rozvoja manažmentu KIB (vypracovanie, aktualizácia a implementácia smerníc a plánov pre rozvoj IT, ...) v organizácii bude zvýšené povedomie zamestnancov o dôležitosti kybernetickej bezpečnosti. Toto je kľúčové pre prevenciu a efektívnu reakciu na incidenty.

Prínosy projektu budú pravidelne monitorované a vyhodnocované počas jeho realizácie aj počas obdobia udržateľnosti, aby sa zabezpečilo, že ciele projektu sú dosiahnuté a prínosy sú trvalé a merateľné.