inFormo s.r.o.
Drobného 27, 841 01 Bratislava
IČO: 35762756, IČ DPH: SK2020273761

Webový portál pre Národný katalóg otvorených dát

Bezpečnostný projekt

Verzia: 29. septembra 2023

Obsah

I. Identifikácia informačného systému

Názov aktíva (siete/IS):	Webový portál pre Národný katalóg otvorených dát
Vlastník aktíva (správca siete/IS):	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
Klasifikačný stupeň z hľadiska DÔVERNOSTI:	Interné
Klasifikačný stupeň z hľadiska INTEGRITY:	Nízka
Klasifikačný stupeň z hľadiska DOSTUPNOSTI:	Nízka
Kategória siete/IS:	I

II. Úvodné ustanovenia

Tento bezpečnostný projekt je súčasťou bezpečnostnej dokumentácie v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti (v kontexte požiadavky §2 ods. (1) písm. a) a zároveň Prílohy č. 1 k vyhláške č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení).

Zároveň je spracovaný v kontexte požiadaviek zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ako aj vyhlášky č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy a taktiež v kontexte požiadaviek medzinárodných noriem radu ISO/IEC 27000.

III. Súvisiace dokumenty

V tejto časti sú uvedené odkazy na iné dokumenty, ktorých informácie súvisia s daným projektom, ale nie sú súčasťou tohto dokumentu (napr. zmluvy s klientom, ponuky, samostatný plán kvality a pod.).

č.	Názov dokumentu
1.	Aplikačná príručka
2.	Konfiguračná príručka a pokyny pre diagnostiku
3.	Havarijný plán

IV. Použité skratky

Skratka	Význam
HW	Skratka pre technické vybavenie informačných systémov, počítačov a počítačových komponentov
IČO	Identifikačné číslo organizácie
IS	Informačný systém
IT	Informačná technológia
LAN	Local area network – lokálna počítačová sieť
Ú OOÚ SR	Úrad na ochranu osobných údajov Slovenskej republiky
OS	Operačný systém
OÚ	Osobné údaje
RDP	Remote Desktop Protocol
SW	Software, programové vybavenie počítačov a ich periférnych zariadení

V. Použitá terminológia

Pojem	Význam
IT špecialista	Pracovník alebo externá firma, majúci(a) kompetenciu spravovať informačné technológie organizácie. Je zodpovedný za riadenie, prevádzku a správu informačných systémov a počítačovej siete vrátane technického a prevádzkového riešenia bezpečnostných aspektov.
Informačné aktíva	Sú najmä objekty, hardvér, softvér, osobné údaje, kvalifikované osoby a ďalšie prvky informačného systému, ktoré prevádzkovateľ považuje za dôležité.
Bezpečnostné riziko	Pravdepodobnosť, že hrozba využije zraniteľnosť aktív, čím nepriaznivo ovplyvní dôvernosť, integritu alebo dostupnosť spracúvaných osobných údajov, ako aj vážnosť dopadu využitia takejto zraniteľnosti.
Bezpečnostný incident	Udalosť majúca za následok ohrozenie dôveryhodnosti osobných údajov (stratou, krádežou, neautorizovaným prístupom atď.) alebo obmedzenie ich dostupnosti.
Technické opatrenia	Systém fyzickej a informačno-technologickej ochrany informačného systému.
Internet	Medzinárodný systém navzájom prepojených počítačových sietí, ktorý umožňuje fungovanie rozličných druhov elektronickej komunikácie.

Pojem	Význam
Vyššia moc	Náhodná, neočakávaná udalosť, vyvolaná rôznymi prejavmi fyzikálnej alebo sociálnej povahy, ktorá nezávisí od pôsobenia organizácie či osoby, napr.: požiar, zatopenie vodou, terorizmus, chrípkové epidémie, komunikačné zlyhania, neidentifikované prírodné vplyvy, atď.
Autentifikácia	Proces, ktorý umožňuje používateľovi pristupovať k privilegovaným údajom. Tento proces zvyčajne končí plne identifikovaným používateľom, čo znamená, že jeho identita sa prenesie poskytovateľovi služieb a poskytovateľ rozpozná používateľa ako klienta, partnera, či entitu v rámci akéhokoľvek prípustného vzťahu.
Autorizácia	Proces, ktorý umožňuje prideliť používateľovi oprávnenia pristupovať k privilegovaným údajom, alebo k operáciám so súbormi po overení identity autentifikáciou.
Neautorizovaná osoba, činnosť, prístup	Osoba, činnosť, prístup a podobne, ktorá nemá v určenom čase príslušné povolenia na vyvolanie danej služby, alebo prístupu k privilegovaným údajom.
Nepovolaná osoba	Osoba, ktorá nemá oprávnenie, poverenie niekde byť, alebo vykonávať istú činnosť a nie je oprávnená oboznamovať sa s chránenými informáciami.

VI. Zoznam právnych predpisov

a) Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,

b) Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,

c) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,

d) Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,

e) STN EN ISO/IEC 27001 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001:2013 vrátane Cor. 1: 2014 a Cor. 2: 2015).

f) STN EN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.

g) STN ISO/IEC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.

VII. Účel dokumentu

Bezpečnostný projekt slúži na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Správca tohto informačného systému chráni spracúvané informácie pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania.

Na tento účel sú prijímané primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania informácií, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných informácií, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému. Prijatím bezpečnostných opatrení správca neoprávneným osobám znemožňuje akýkoľvek nedovolený prístup k spracúvaným informáciám a oprávneným osobám zabezpečí prístup k informáciám v rozsahu potrebnom na plnenie ich povinností.

VIII. Ciele bezpečnostného projektu informačného systému

Tento Bezpečnostný projekt platí pre konkrétny informačný systém (ďalej aj „IS“) v správe organizácie. Za udržiavanie a aktuálnosť tohto bezpečnostného projektu zodpovedá správca IS.

Cieľom tohto bezpečnostného projektu IS je definovanie základných rámcov ochrany informácií spracúvaných počas celého ich životného cyklu, t.j. od ich získavania až po ich likvidáciu, so zabezpečením súladu spracúvania osobných údajov s legislatívou SR, ako aj dôvernosti, integrity a dostupnosti informácií.

Súčasťou tohto bezpečnostného projektu informačného systému je kvalitatívna analýza rizík. Analýzou rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva. Analýzou rizík sa tiež identifikujú a ohodnocujú riziká, ktoré majú alebo môžu mať na chránené informačné aktíva vplyv. Výstupy takejto analýzy pomôžu v rozhodovaní vedeniu organizácie a zodpovedných pracovníkov pri aplikovaní bezpečnostných opatrení.

Pre potreby analýzy rizík sa zoznam hrozieb môže združiť do jednotlivých skupín tak, že je možné tento zoznam použiť univerzálne pre väčšinu aktív. Pre jednotlivé aktíva sú hodnotené len hrozby relevantné pre konkrétne aktívum. Analýza rizík slúži na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti. Analýza rizík je hlavnou časťou bezpečnostného projektu v kontexte požiadaviek zákona č. 95/2019 Z. z. a jeho vykonávacích predpisov pre potreby informačného systému verejnej správy.

Bezpečnostný projekt IS definuje formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov organizácie, technických noriem a štandardov dobrej praxe (obsahuje komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek, návrh spôsobu ich

efektívneho naplnenia a vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika).

Na dosiahnutie primeranej úrovne ochrany informácií v informačnom systéme je potrebné navrhnúť a implementovať také technické, organizačné a personálne opatrenia, aby bola zabezpečená ochrana vstupných dokladov, ochrana spracúvania informácií automatizovaným spôsobom, narábanie s informáciami oprávnenými osobami, zamedzenie prístupu k informáciám neoprávneným osobám, ochrana a bezpečná likvidácia dokumentov a dokumentov uložených na elektronických médiách, v registratúrach a archívoch.

Minimálne požadované bezpečnostné opatrenia sú:

a) riadenie prístupu k informáciám na ochranu pred neoprávneným prístupom,

b) zabezpečenie realizovaných činností zverejňovania otvorených dát v predmetnom IS,

c) monitorovanie činností pri spracúvaní informácií a riadení činností v predmetnom IS.

IX. Bezpečnostný zámer

Ako prvý výstup bezpečnostného projektu informačného systému verejnej správy sa vypracuje dokument „Bezpečnostný zámer“. Bezpečnostný zámer určuje najmä kontext a zameranie bezpečnostného projektu, preto v súlade s legislatívou (Príloha č. 3 k vyhláške č. 179/2020 Z. z.) obsahuje najmenej:

a) formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov orgánu riadenia, technických noriem a štandardov dobrej praxe,

b) zoznam právnych predpisov aplikovaných v bezpečnostnom projekte, ako aj interných riadiacich aktov,

c) metodický prístup ku kvalitatívnej analýze rizík, ktorá je v bezpečnostnom projekte vykonaná,

d) rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany informačného systému verejnej správy, jeho služieb a údajov v ňom spracúvaných s ohľadom na kategóriu, do ktorej je informačný systém verejnej správy zaradený,

e) vymedzenie okolia informačného systému verejnej správy a jeho vzťah k možnému narušeniu bezpečnosti informačného systému verejnej správy vrátane zoznamu integrácií na informačný systém verejnej správy,

f) vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,

g) ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo projektu informačného systému verejnej správy),

h) postupy revízie/aktualizácie bezpečnostného zámeru.

X. Analýza bezpečnosti

Ako druhý hlavný výstup bezpečnostného projektu informačného systému verejnej správy sa vypracuje dokument „Analýza bezpečnosti“, ktorého súčasťou je kvalitatívna analýza rizík. Rizikom sa v bezpečnostnom projekte chápe miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami.

A. Analýza rizík

Analýza rizík je zameraná na získanie aktuálnych a vierohodných poznatkov o pravdepodobných rizikách týkajúcich sa aktív informačného systému verejnej správy a jeho okolia. Analýza rizík sa vykonáva pre informačný systém verejnej správy priebežne počas celého projektu v súlade so zákonom č. 95/2019 Z. z. a priamo nadväzuje na dokument „Bezpečnostný zámer“.
Metodický postup výkonu analýzy rizík musí byť v súlade s technickou normou (napr. STN ISO/IEC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti (ISO/IEC 27005)).
Výsledné vyhodnotenie rizík podľa použitej metodiky musí byť premietnuté do trojstupňovej stupnice nízke riziko, stredné riziko, vysoké riziko.
Pri tvorbe navrhovaných bezpečnostných opatrení je potrebné určiť prostriedky a procesy odstraňovania nedostatkov zistených v rámci jednotlivých rizík. Cieľom návrhu bezpečnostných opatrení je vytvorenie takého okruhu bezpečnostných opatrení, že po ich implementácii a následnom prehodnotení rizík sú všetky zvyškové riziká akceptovateľné. Pri niektorých typoch opatrení je prípustné sa odkazovať aj na dokumentáciu k informačnému systému verejnej správy v súlade so zákonom č. 95/2019 Z. z..

Pre konkrétne aktíva organizácie je vypracovaná analýza rizík v súlade s požiadavkou zákona č. 95/2018 Z.z. a normou STN ISO/IEC 27005 Riadenie rizík informačnej bezpečnosti v nasledujúcom rozsahu:

- Identifikácia a klasifikácia aktív IS.
- Identifikácia hrozieb a zraniteľností pre IS.
- Ohodnotenie rizík pre IS.
- Identifikácia a ohodnotenie doteraz realizovaných bezpečnostných opatrení.
- Porovnanie aktuálneho stavu bezpečnosti v IS s požiadavkami STN ISO/IEC 27002.
- Návrh možných bezpečnostných opatrení pre minimalizáciu identifikovaných rizík.
- Hodnotenie použitých opatrení a návrh opatrení na identifikované zraniteľnosti sú v súlade s normou STN ISO/IEC 27002.

Pre analýzu rizík bola zvolená metóda kvalitatívnej analýzy rizík.

a) Ohraničenia aktíva, pre ktoré je analýza rizík spracovaná

Webový portál pre Národný katalóg otvorených dát.

b) Identifikácia aktív

V tomto kroku analýzy sa vykoná identifikovanie každého relevantného aktíva. Klasifikácia aktív vyjadruje dôležitosť daného aktíva pre organizáciu. Je možné ho vyjadriť z dôsledkov možných nepriaznivých dopadov na činnosť organizácie v prípade modifikácie, nedostupnosti, zničenia informácií systému alebo z narušenia dôvernosti. V postupe klasifikácie aktív je zohľadnená ich vzájomná závislosť a z toho plynúca možnosť vplyvu na samotnú prevádzku IS.

Kvôli prehľadnosti môže byť zavedené rozdelenie identifikovaných aktív na primárne a podporné aktíva v súlade s požiadavkou STN ISO/IEC 27005. Aktíva v prostredí organizácie je možné rozdeliť podľa odporúčaní prílohy B normy STN ISO/IEC 27005na hlavné a podporné.

Výsledkom plynúcim z kvalitatívneho ohodnotenia môže byť úroveň dôležitosti aktíva vyjadrená v nefinančných hodnotách.

c) Klasifikácia aktív

Pre potreby tejto analýzy *je vytvorená trojúrovňová stupnica na ohodnotenie aktív*. Jednotlivé aktíva sú podľa ich významu klasifikované podľa podmienok klasifikácie zákona č. 69/2018 Z.z. Vo vytvorenej klasifikačnej schéme sa pre ohodnotenie aktíva spoločne uplatňujú podmienky dôvernosti, dostupnosti a integrity.

1. **Vysoko významné (V)** – sem patria aktíva klasifikované do kategórie III a informácie z hľadiska dôvernosti v klasifikačnom stupni Chránené a Prísne chránené, ostatné aktíva, ak so zlyhaním aktíva alebo únikom informácií sú spojené značné náklady, ak obnova aktíva nie je jednoduchá a nedá sa krátkodobo nahradiť iným aktívom. Aktívum má malú toleranciu na neplánovaný výpadok – rádovo niekoľko hodín a ktorého chyba, nepresnosť bezprostredne ohrozuje poskytovanú službu, s ňou spojené aktivity a reputáciu prevádzkovateľ.
2. **Významné (S)** – sem patria aktíva klasifikované do kategórie II a informácie z hľadiska dôvernosti v klasifikačnom stupni Interné a ostatné aktíva, ak so zlyhaním aktíva alebo únikom informácií sú spojené značné náklady, ak obnova aktíva je jednoduchá, alebo sa dá krátkodobo nahradiť iným aktívom. Aktívum má strednú toleranciu na neplánovaný výpadok – približne 2-3 dni a ktorého chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovaných služieb, strategickú oblasť a prevádzkové riziká.
3. **Málo významné (N) –** sem patria aktíva klasifikované do kategórie I a informácie z hľadiska dôvernosti v klasifikačnom stupni Verejné a ostatné aktíva, ak aktívum sa dá ľahko nahradiť, únik informácií nespôsobí ujmu. Aktívum má veľkú toleranciu na neplánovaný výpadok – rádovo viacero dní a ktorého chyba alebo nepresnosť výrazne neohrozí poskytovanú službu.

d) Identifikácia a ohodnotenie hrozieb

V tejto časti je potrebné spracovať všeobecný katalóg hrozieb, ktorý zahŕňa všetky identifikované hrozby s možným negatívnym pôsobením na činnosť informačného systému. Sú zvažované hrozby prírodného, ako aj ľudského pôvodu (hrozby logického, fyzického a politického charakteru). V katalógu bezpečnostných hrozieb sa uvažuje s náhodným, ako aj úmyselným zdrojom realizácie hrozby. Inšpiráciou pre katalóg hrozieb môže byť príklad typických hrozieb uverejnených v STN ISO/IEC 27005 a zoznam najviac pôsobiacich hrozieb za aktuálny rok napr. podľa ENISA.

e) Identifikácia a ohodnotenie bezpečnostných zraniteľností podľa hrozieb pôsobiacich na aktíva

Cieľom nasledujúceho kroku je špecifikácia a ohodnotenie zraniteľností (slabých miest) v postupoch, manažmente, organizácii, personálnej oblasti, hardvéri, softvéri, komunikačnom zariadení a vo fyzickom prostredí, ktoré môžu byť využité hrozbami.

Zraniteľnosť konkrétneho aktíva je určovaná vo vzťahu ku každej hrozbe osobitne, ktorá by mohla túto zraniteľnosť v špecifickej situácii využiť. Identifikácia zraniteľností je vykonaná prostredníctvom príkladov zraniteľností uvedených v STN ISO/IEC 27005, podľa znalostí a zverejnených slabín použitých technológií v informačnom systéme a využitých organizačných opatrení na riadenie informačnej bezpečnosti posudzovaného systému.

Na ohodnotenie zraniteľnosti identifikovaných aktív môže byť použitá klasifikácia uvedená v priloženej tabuľke (hodnota zraniteľnosti je posudzovaná pri pôsobení konkrétnej hrozby bez zohľadnenia doteraz implementovaných opatrení, s ohľadom na aktuálne implementované opatrenia a po návrhu opatrení):

Ohodnotenie	Popis ohodnotenia zraniteľnosti
Veľmi Vysoká	Výskyt zraniteľnosti degraduje bezpečnosť resp. funkčnosť IS.
Vysoká	Výskyt zraniteľnosti významne znižuje bezpečnosť resp. funkčnosť IS.
Stredná	Výskyt zraniteľnosti znižuje bezpečnosť resp. funkčnosť IS.
Nízka	Výskyt zraniteľnosti neznižuje vo významnej miere bezpečnosť alebo resp. funkčnosť IS.

f) Ohodnotenie rizík

Cieľom tejto časti je identifikovať a odhadnúť riziká, ktorým je konkrétny IS vystavený. Riziko je stanovené na základe hodnoty aktíva, pravdepodobnosti hrozby, ktorá spôsobí potenciálne nepriaznivé dopady na činnosť organizácie a hodnoty identifikovaných zraniteľností.

Na základe hodnoty aktuálneho rizika by mali byť vybraté vhodné bezpečnostné ochranné opatrenia v súlade s STN ISO/IEC 27002. Táto hodnota miery rizika stanovuje základ pre návrh opatrení, ktoré budú prioritne použité na minimalizáciu rizík spôsobujúcich najnepriaznivejšie dopady.

Miera rizika predstavuje pravdepodobnosť, že daná hrozba využije zraniteľnosť aktíva alebo skupiny aktív a spôsobí tak nežiadúci dopad na aktívum.

Miera rizika môže byť rozčlenená do nasledovných stupňov:

a) Veľmi vysoká (VV),
b) Vysoká (V),
c) Stredná (S),

d) Nízka (**N**),

g) Samotná analýza rizík (Výstupný dokument analýzy rizík)

I. Neautorizovaný prístup k údajom

Autentifikáciu pre analyzovaný portál zabezpečuje ÚPVS, ale autorizáciu vykonáva samostatný interný komponent portálu. Neautorizovaný prístup k dátam je v prípade webového portálu NKOD primárne taký, ktorý pôsobí neautorizovanú zmenu poskytovaných dát.

Zraniteľnosť: stredná

Miera rizika: nízka

II. Odopretie prístupu, nedostupnosť služby

Portálové riešenie je dostupné, ak sú splnené všetky požiadavky na jeho prevádzku a sú k dispozícii dostatočné zdroje na realizáciu nevyhnutných činností spojených s prevádzkou. Zabezpečenie týchto zdrojov je riešené mimo portálového riešenia využitím cloudových služieb v dostatočnej kapacite.

Zraniteľnosť: nízka

Miera rizika: nízka

III. Havária

Havária IS vzniká z dôvodu hardvérového, softvérového alebo personálneho zlyhania. Keďže je portálové riešenie súčasťou dodávky softvéru je nevyhnutné predchádzať udalostiam, ktoré majú za následok celkové alebo čiastočné zlyhanie poskytovaných služieb.

Zraniteľnosť: stredná

Miera rizika: nízka

IV. Injekcia neautorizovaného kódu

Injekcia neautorizovaného kódu ohrozuje prevádzkované aplikácie na strane servera a klienta. Môže vzniknúť na základe používateľského vstupu vytvoreného na tento účel, vložením kódu do repozitárov, z ktorých je aplikácia zostavovaná alebo využitím kódu tretej strany, ktorý je zraniteľný alebo úmyselne napadnutý.

Zraniteľnosť: stredná

Miera rizika: stredná

V. Zlyhanie kryptografického riešenia

Pre autorizáciu prístupu k údajom sa používa kryptografická metóda RSA vo veľkosti 2048 bitov a v prípade dostatočnej entropie pri generovaní kľúčov ju možno považovať za štandard považovaný aktuálne za neprelomiteľný.

Zraniteľnosť: stredná

Miera rizika: nízka

VI. Nesprávna konfigurácia

Konfigurácia komponentov portálu obsahuje nastavenie, ktoré majú na miestu bezpečnosti zásadný vplyv. Neautorizovaný prístup ku konfigurácií znamená vážne ohrozenie bezpečnosti ponúkaných služieb. Z týchto dôvodov je nutné obmedziť prístup k prostriedkom, v ktorých je konfigurácia nevyhnutne potrebná alebo uložená.

Zraniteľnosť: vysoká

Miera rizika: nízka

VII. Využívanie komponentov so známymi zraniteľnosťami

Portálové riešenie priamo využíva softvérové komponenty tretích strán v podobe produktov s otvoreným zdrojovým kódom, ktoré sú využívané vo veľkom množstve iných projektov. Ich prípadná zraniteľnosť v prípade zverejnenia môže mať širokú dosah na odbornú a laickú verejnosť a vzhľadom na zverejnené zdrojové kódy riešenia môže dôjsť k reálnemu využitiu zraniteľnosti portálu.

Zraniteľnosť: vysoká

Miera rizika: nízka

Návrh bezpečnostných opatrení

Pre konkrétnu hrozbu, ktorá pôsobí na aktívum prostredníctvom identifikovaných zraniteľností musia byť navrhnuté relevantné opatrenia tak, aby bola každá zraniteľnosť resp. skupina zraniteľností pokrytá konkrétnym opatrením:

Opatrenia	Opis opatrenia	Aktuálne riziko	Zvyškové riziko
Opatrenie k Z I: Neautorizovaný prístup k údajom	Monitorovanie, logovanie a auditovanie (v prípade potreby) všetkých informácií o prístupe autentifikovaných používateľov a aktívnych prístupoch k dátam	nízke	nízke
Opatrenie k Z II: Odopretie prístupu, nedostupnosť služby	Vykonávanie dohľadu nad použitými cloudovými službami v dostatočnej kapacite	nízke	nízke
Opatrenie k Z III: Havária	Monitoring prevádzkových prostriedkov	nízke	nízke

	a pravidelné vyhodnocovanie udalostí		
Opatrenie k Z IV: Injekcia neautorizovaného kódu	Dohľad nad vykonávaním validácie a sanitácie používateľských vstupov, používanie len oficiálny a bezpečných zdrojov softvéru	stredné	nízke
Opatrenie k Z V: Zlyhanie kryptografického riešenia	Monitoring situácie v oblasti kryptografie	nízke	nízke
Opatrenie k Z VI: Nesprávna konfigurácia	Validácia konfigurácie v režime 4 oči	nízke	nízke
Opatrenie k Z VII: Využívanie komponentov so známymi zraniteľnosťami	Pravidelné sledovanie vydaných nových verzií, resp. ich aktualizácia min. 1x mesačne	nízke	nízke

h) Vymedzenie kritérií na akceptáciu rizika

Akceptovateľné riziká sú všetky, ktorých miera rizika je **Nízka**. U týchto nie je potrebné uplatniť ďalšie opatrenia, prípadne prehodnotiť pôsobenie rizika.

Každé riziko s mierou rizika **Stredná** musí byť osobitne posúdené vzhľadom na jeho pôsobenie, škálu navrhovaných opatrení a cenu opatrení na jeho akceptovateľnú úroveň.

Riziká s mierou rizika **Vysoká** alebo **Veľmi vysoká** je potrebné zabezpečiť navrhovanými opatreniami až na akceptovateľnú úroveň, prípadne na úroveň miery rizika Stredná s uplatnením pravidiel pre riziká s mierou rizika Stredná.

i) Určenie nepokrytých rizík

Po vykonaní analýzy rizík a návrhu ochranných opatrení je potrebné zabezpečiť akceptáciu nepokrytých a zostatkových rizík. Žiadny systém nie je absolútne bezpečný, preto vždy budú existovať zostatkové riziká. Tieto by mala organizácia rozdeliť na **prijateľné** a **neprijateľné**.

Neprijateľné by nemali byť bez ďalšieho posúdenia tolerované. Je vecou vedenia či budú akceptované z titulu ďalšieho obmedzenia (nemožnosť prevencie, napr. v prípade zemetrasenia). V týchto prípadoch však môžu byť realizované plány obnovy z takýchto udalostí, prípadne poistenie, alebo či budú prijaté k zníženiu neprijateľných rizík vybrané dodatočné a možno aj finančne nákladné ochranné opatrenia.

XI. Postupy revízie tejto analýzy rizík

Revízia analýzy rizík sa vykonáva v súlade s požiadavkou na vykonávanie analýzy rizík a vyhodnocovanie súladu implementovaných opatrení s Vyhláškou č.197/2020 Z.z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (a ďalšou platnou relevantnou legislatívou predpismi v oblasti kybernetickej a informačnej bezpečnosti). Vyhláška predpokladá revíziu analýzy rizík minimálne raz za 12 mesiacov.

Revízia analýzy rizík sa vykoná aj v rámci kratšej periódy, ak došlo k narušeniu dôvernosti alebo integrity Chránených alebo Prísne chránených informácií, ako aj pri zásadnej zmene funkčnosti aktíva, ktorá má vplyv na spracúvanie Chránených a Prísne chránených informácií.

XII. Záverečné ustanovenia

Tento dokumentu musí byť revidovaný a vyhodnocovaný minimálne raz ročne. Dokument je záväzný pre všetkých zamestnancov organizácie prichádzajúcim akýmkoľvek spôsobom do styku s konkrétnym informačným systémom, ktorého sa týka.