Metodické usmernenie z 11.10.2023 č. 023107/2023/oSBATA-1 pre klasifikáciu informačných systémov verejnej správy podľa typu údajov, s ktorými pracujú a ukladajú

Určené pre:	Sekcia informačných technológií verejnej správy, orgány riadenia podľa § 5 ods. 2 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Vydáva:	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky Sekcia informačných technológií verejnej správy
Záväznosť:	Tento dokument má odporúčací charakter
Počet príloh:	2
Dátum vydania:	11.10.2023
Dátum účinnosti:	16.10.2023
Schválil:	Mgr. Ildikó Štúňová, poverená riadením sekcie informačných technológií verejnej správy Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Obsah

1. Úvod

Cieľom tohto metodického usmernenia je zadefinovanie postupu v orgánoch riadenia (ďalej len „OR“) pre určenie klasifikačných parametrov informačných systémov verejnej správy (ďalej len „ISVS“) a ISVS, ktoré sú základnou službou alebo súčasťou základnej služby, a to v súlade legislatívnymi predpismi v časti 1.1. Legislatíva.

Výsledná klasifikácia ISVS – Ux(CxIxAx) určená pomocou tohoto metodického usmernenia pomôže OR pri výbere a obstarávaní cloudových služieb pre prevádzku ISVS.

1.1. Legislatíva

- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“),
- 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 v znení vyhlášky Národného bezpečnostného úradu č. 264/2023 Z. z. (ďalej len „vyhláška NBÚ č. 362/2018 Z. z.”),
- zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 95/2019 Z. z.“),
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov,
- vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (ďalej len „vyhláška NBÚ č. 165/2018 Z. z.”),
- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 215/2004 Z. z.”),
- ďalšie súvisiace predpisy.

2. Vymedzenie základných pojmov

2.1. ISVS ako aktívum

Aktívum je v oblasti informačnej bezpečnosti čokoľvek, čo je nutné z pohľadu organizácie chrániť.

- aktívom je **ISVS**,
- aktívom sú podľa § 3 písm. u) zákona č. 95/2019 Z. z. programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaná osoba, dobré meno OR a informácia, dokumentácia, zmluva a iná skutočnosť, ktorú považuje OR za citlivú.

2.2. Informačný systém

Informačným systémom je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.

2.3. Informačné aktíva

Informačným aktívom sú informácie, údaje, ktoré je nutné z pohľadu organizácie chrániť (ďalej len „informačné aktíva“).

2.4. Klasifikácia informačných aktív

Klasifikačné stupne opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív z pohľadu narušenia ich dôvernosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív.

Klasifikácia posúdenia potrieb ochrany informačných aktív (v tomto prípade aj ISVS) z hľadiska dostupnosti, dôvernosti, integrity, autentickosti a ich následné zaradenie do klasifikačnej kategórie (triedy) zodpovedajúcej týmto potrebám.

Podľa prílohy č. 1 vyhlášky NBÚ č. 362/2018 Z. z. sa informačné systémy klasifikujú nasledujúcimi klasifikačnými stupňami:

1. Klasifikačné stupne z hľadiska **dôvernosti (C -** confidentiality**)**:

- Verejné,
- Interné,
- Chránené,
- Prísne chránené.

2. Klasifikačné stupne z hľadiska **integrity (I -** integrity**)**:

- Nízka,
- Stredná,
- Vysoká.

3. Klasifikačné stupne z hľadiska **dostupnosti (A -** availability**)**:

- Nízka,
- Stredná,
- Vysoká.

2.5. Kategorizácia informačných systémov a sietí

Rozdelenie informačných systémov a sietí do kategórií sa uskutočňuje podľa klasifikačných kritérií definovaných v prílohe č. 1 k vyhláške NBÚ č. 362/2018 Z. z. , t. j. do nasledovných kategórií:

- Kategória I.,
- Kategória II.,
- Kategória III.

2.6. Klasifikované informačné aktívum – informácia

Klasifikovaným informačným aktívom je také aktívum, ktorého ochrana vyplýva z platnej legislatívy Slovenskej republiky (podľa časti 1.1. Legislatíva). Pri jeho odovzdávaní inému organizačnému útvaru alebo tretej strane, vlastník informačného aktíva zabezpečuje s odovzdaním aj oznámenie o druhu (kategória a klasifikačné stupne) informačného aktíva a spôsobe narábania s informačným aktívom.

2.7. Klasifikácia a kategorizácia ISVS

V tomto metodickom usmernení hovoríme aj o kategorizácii a klasifikácii ISVS (ako aktíva), ktoré pracuje s informačnými aktívami a preberá tieto parametre z informačných aktív.

2.8. Pojmy súvisiace s informačným aktívom

Vlastník informačného aktíva

Vlastníkom informačného aktíva je OR a poverená osoba kompetenčne zodpovedná za požadovanú úroveň ochrany informačných aktív, ktoré sú v jej organizačnej pôsobnosti spracúvané, primárne za účelom zabezpečenia chodu procesov.

Typickými vlastníkmi informačných aktív sú OR a zodpovednosť je u vedúcich pracovníkov vymedzená interným predpisom.

Oprávnená osoba v časti klasifikácia informačných aktív

Oprávnenou osobou je osoba, ktorá je určená vlastníkom informačného aktíva na spracúvanie alebo/a oboznamovanie sa s vymedzeným rozsahom informačného aktíva alebo jej oprávnenie vyplýva zo zákona, resp. z výkonu jej pracovnej pozície (funkcie).

Nepovolaná osoba v časti klasifikácia informačných aktív

Nepovolanou osobou je osoba, ktorá nie je určená na spracúvanie alebo/a oboznamovanie sa s informačnými aktívami zaradenými v systéme ochrany alebo rozsah jej určenia nie je postačujúci.

Vedenie organizácie

Osoba, ktorá zabezpečuje proces vedenia organizácie (t. j. OR) a zodpovedá za priebeh tohto procesu. Pod vedením organizácie môžeme rozumieť vedenie organizácie ako celku, ako aj jej jednotlivých organizačných útvarov.

Iný poverený zamestnanec

Zamestnanec určený vedením organizácie na vykonávanie špecifických úloh organizácie.

Dôvernosť, integrita a dostupnosť informačných aktív

Dôvernosť (**C -** confidentiality) je záruka, že údaj nie je vyzradený neoprávneným subjektom alebo procesom.

Integrita (**I -** integrity) je záruka, že bezchybnosť, úplnosť alebo správnosť údajov nie sú narušené.

Dostupnosť (**A -** availability) je záruka, že údaj je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj potrebný a požadovaný.

3. Roly, zodpovednosti a právomoci

3.1. Roly, zodpovednosti a právomoci v rámci klasifikácie informačných aktív, informácií

Vlastníci informačného aktíva zodpovedajú za evidenciu a triedenie informačných aktív do klasifikačných stupňov podľa klasifikačnej schémy (pozri nasledujúcu kapitolu).

Klasifikácia a evidencia informačných aktív sú vykonávané aspoň raz ročne a vždy v prípade, ak:

- nastane zmena v spravovaní informačných aktív,
- nastane zmena v súvisiacich právnych predpisoch,
- vznikne nový typ dokumentu obsahujúci informačné aktíva, ktoré vyžadujú klasifikáciu.

Vedenie organizácie alebo iný poverený zamestnanec:

- zodpovedajú za riadenie a výkon ochrany informačných aktív,
- zabezpečujú aktuálnosť klasifikácie informačných aktív,
- vyhodnocujú správnosť klasifikácie informačných aktív v súlade s definovanou klasifikačnou schémou,
- kontrolujú súlad ochrany informačných aktív podľa definovaných bezpečnostných požiadaviek klasifikačnej schémy.

Povereným zamestnancom sa myslí najmä manažér kybernetickej bezpečnosti organizácie určený podľa zákona č. 69/2018 Z. z.

Za výkon ochrany podľa tohto dokumentu zodpovedajú taktiež osoby prichádzajúce do styku s klasifikovanými a/alebo neklasifikovanými informačnými aktívami.

Vedenie organizácie alebo iný poverený zamestnanec, v ktorého pôsobnosti sú vzťahy s verejnosťou, zodpovedajú za výber, postup a rozsah poskytovania verejne prístupných informačných aktív.

Zamestnanci organizácie sú povinní ochraňovať, t. j. nezverejňovať, neposkytovať ani nesprístupňovať nepovolanej osobe všetky klasifikované i neklasifikované informačné aktíva, s ktorými pri plnení svojich pracovných povinností prichádzajú do styku, a to aj v prípade, že nie sú oprávnenou osobou.

3.2. Roly, zodpovednosti a právomoci v rámci kategorizácie informačných systémov a sietí

Kategorizácia informačných systémov a sietí je vykonávaná minimálne raz za rok a vždy v prípade, ak:

- nastane zásadná zmena v sieti alebo informačnom systéme,
- nastane zmena v súvisiacich právnych predpisoch,
- do produkčnej prevádzky bude uvedená nová sieť alebo informačný systém.

Vedenie organizácie alebo iný poverený zamestnanec:

- zodpovedajú za riadenie a výkon kategorizácie sietí a informačných systémov,
- zabezpečujú aktuálnosť kategorizácie sietí a informačných systémov,
- vyhodnocujú správnosť kategorizácie sietí a informačných systémov v súlade s definovanou kategorizačnou schémou.

Povereným zamestnancom je najmä manažér kybernetickej bezpečnosti organizácie určený podľa zákona č. 69/2018 Z. z.

Zamestnanci organizácie sú povinní rešpektovať platnú kategorizáciu sietí a informačných systémov a to aj v prípade, že nie sú oprávnenou osobou.

4. Metodika klasifikácie informačných aktív

Informačné aktíva sa v rámci organizácie vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Každé klasifikované informačné aktívum má pridelený jeden klasifikačný stupeň dôvernosti, jeden klasifikačný stupeň integrity a jeden klasifikačný stupeň dostupnosti.

Bezpečnostné informačné aktíva, nastavenia, postupy, smernice a ostatné úkony týkajúce sa riadenia aktív sa klasifikujú rovnakým alebo vyšším klasifikačným stupňom, akým sú označené informačné aktíva, ktorých riadenie opisujú.

Pri klasifikácii informačných aktív sa uplatňuje odstupňovaný prístup tak, že do nižších úrovní sú zahrnuté také informačné aktíva, pri ktorých sú najnižšie nároky na dôvernosť, integritu, dostupnosť a zodpovednosť vrátane zabezpečovania kvality. Informačné aktíva sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Organizácia môže na základe racionálneho zváženia skutkového stavu, dostatočného odôvodnenia a schválenia manažérom kybernetickej a informačnej bezpečnosti a relevantným vedúcim pracovníkom jednotlivé informačné aktíva zaradiť do vyššieho alebo nižšieho stupňa ako vyplýva z vykonanej klasifikácie.

Klasifikačné stupne opisujú citlivosť informačných aktív, údajov alebo ďalších s nimi spojených informačných aktív a odrážajú dôležitosť alebo hodnotu týchto aktív pre organizáciu z pohľadu narušenia ich:

- dôvernosti,
- integrity,
- dostupnosti.

Dotazník slúžiaci na určenie klasifikačných stupňov jednotlivých informačných aktív je súčasťou prílohy č. 1.

4.1. Klasifikačné stupne z pohľadu dôvernosti

Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované v prílohe č. 2 vyhlášky NBÚ č. 362/2018 Z. z. nasledovnými spôsobmi:

4.1.1 Klasifikačný stupeň – Prísne chránene

Prísne chránené informačné aktíva sú informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom organizácie, a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na organizáciu. Prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je umožnený výhradne konkrétnej, vopred určenej a schválenej osobe. Tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov (časť 1.1. Legislatíva).

4.1.2 Klasifikačný stupeň – Chránené

Chránené informačné aktíva sú informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre organizáciu negatívny vplyv. Prístup k údajom klasifikovaným ako „chránené“ je riadený

pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je umožnený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb. Tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom.

4.1.3 Klasifikačný stupeň – Interné

Interné informačné aktíva sú informačné aktíva, ktoré majú výpovednú hodnotu a význam pre organizáciu, preto sú určené len pre vnútornú potrebu organizácie, sú používané a prístupné pre všetkých používateľov v rámci organizácie bez ohľadu na ich pracovnú rolu. Na sprístupnenie týchto informačných aktív tretím stranám je potrebné schválenie zo strany vlastníka informačného aktíva. Vyžadujú si základnú úroveň ochrany.

4.1.4 Klasifikačný stupeň – Verejné

Verejné informačné aktíva sú informačné aktíva určené pre vonkajšiu komunikáciu a tretie strany, sú získateľné z verejných zdrojov alebo z informačných aktív, ktoré sú pripravené na tento účel, alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie.

4.2. Klasifikačné stupne z pohľadu integrity

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované v prílohe č. 2 vyhlášky NBÚ č. 362/2018 Z. z. nasledovným spôsobom:

4.2.1 Klasifikačný stupeň – Vysoká

Tento stupeň zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť organizácie, a ktorých chyba alebo nepresnosť bezprostredne ohrozuje činnosť organizácie, s ňou spojené aktivity a reputáciu.

Neautorizovaná modifikácia údajov alebo ich nepresnosť, resp. neúplnosť môže mať veľmi vážny dopad na kritické procesy alebo aktíva organizácie s možným výskytom efektu kumulácie viacerých nepriaznivých dopadov.

4.2.2 Klasifikačný stupeň – Stredná

Tento stupeň zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť organizácie, a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu činností organizácie alebo strategickú oblasť, v ktorej organizácia vykonáva svoje aktivity.

Neautorizovaná modifikácia údajov alebo ich nepresnosť, resp. neúplnosť môže mať nepriaznivý dopad na procesy alebo aktíva organizácie, s možným výskytom efektu kumulácie viacerých nepriaznivých dopadov.

4.2.3 Klasifikačný stupeň – Nízka

Tento stupeň zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanie činností zo strany organizácie.

Neautorizovaná modifikácia údajov alebo ich nepresnosť, resp. neúplnosť nemá významnejší nepriaznivý dopad na procesy alebo aktíva organizácie.

4.3. Klasifikačné stupne z pohľadu dostupnosti

Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované nasledovným spôsobom:

4.3.1 Klasifikačný stupeň – Vysoká

Tento klasifikačný stupeň zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť organizácie, a ktorých zlyhanie bezprostredne ohrozuje poskytovanie služieb zo strany organizácie, s ňou spojené aktivity a dobrú povesť organizácie.

4.3.2 Klasifikačný stupeň - Stredná

Tento klasifikačný stupeň zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť organizácie, a ktorých zlyhanie môže mať dopad na kontinuitu poskytovania služieb zo strany organizácie, strategickú oblasť, trhové a operačné riziká.

4.3.3 Klasifikačný stupeň – Nízka

Tento klasifikačný stupeň zahŕňa informačné aktíva organizácie, ktorých výpadok výrazne neohrozí služby poskytované zo strany organizácie, alebo pre ktoré existujú alternatívne postupy.

5. Kategorizácia sietí a informačných systémov

Kategorizácia sietí a informačných systémov (ISVS) je v rámci organizácie založená na klasifikácii informačných aktív podľa prílohy č. 2 vyhlášky NBÚ č. 362/2018 Z. z. (pozri časť 4 metodického usmernenia).

Kategorizácia sa vykonáva pre každú sieť a informačný systém vytvorením zoznamu vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy, ich podporné systémy a podsystémy s uvedením ich bezpečnostnej funkcie a zaradenia do príslušných bezpečnostných kategórií.

Organizácia môže na základe racionálneho zváženia skutkového stavu, dostatočného odôvodnenia a schválenia manažérom kybernetickej a informačnej bezpečnosti a relevantným vedúcim pracovníkom jednotlivé siete a informačné systémy zaradiť do vyššieho alebo nižšieho stupňa ako vyplýva z vykonanej kategorizácie.

Zoznam komponentov sietí a informačných systémov organizácie identifikujúci jednotlivé siete a informačné systémy sa môže skladať z textovej, tabuľkovej a grafickej časti tak, že sú jednoznačne definované:

- hranice vybranej siete a informačného systému,
- rozhrania medzi definovanými hranicami,
- bezpečnostné funkcie komponentov, ktoré majú byť zahrnuté v posudzovaní úrovne bezpečnosti,
- požiadavky príslušných regulačných požiadaviek a technických noriem alebo iných vecne obdobných postupov a metód na ich:
    - projektovanie,
    - vytváranie,
    - implementáciu,
    - kontrolu.

Siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaraďujú do vyššej bezpečnostnej kategórie.

Kategorizácia sietí a informačných systémov zohľadňuje, že zlyhanie siete alebo informačného systému v ľubovoľnej bezpečnostnej úrovni nespôsobí zlyhanie vybranej siete a informačného systému zaradeného do bezpečnostnej úrovne s vyššou kategóriou. Pomocné siete a informačné systémy a podsystémy, ktoré pomáhajú funkciám vybraných informačných systémov, musia byť zaradené do príslušnej bezpečnostnej kategórie s ohľadom na zaradenie nadradeného systému.

V rámci organizácie sa rozoznávajú tri kategórie sietí a informačných systémov:

- kategória I,
- kategória II,
- kategória III.

5.1. Kategórie sietí a informačných systémov

5.1.1 Kategória I.

Kategória I. zahŕňa informačné aktíva v pôsobnosti organizácie:

- **ktorých ohrozenie nemá žiadny negatívny dopad na poskytovanú základnú službu (podľa zákona č. 69/2018 Z. z.)**,
- ktoré sú klasifikované z hľadiska **dôvernosti** ako verejné alebo v odôvodnených prípadoch interné,
- ktoré sú klasifikované z hľadiska **dostupnosti** klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,
- ktoré sú klasifikované z hľadiska **integrity** klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,
- pri ktorých nie je predpoklad potreby identifikácie zodpovednosti za aktivity používateľov,
- pri ktorých nie je potrebné vykonávať kontrolnú činnosť.

5.1.2 Kategória II.

Kategória II. zahŕňa informačné aktíva v pôsobnosti organizácie:

- **ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident I. stupňa (podľa vyhlášky NBÚ č. 165/2018 Z. z.),**
- ktoré sú klasifikované z hľadiska **dôvernosti** ako interné, chránené alebo v odôvodnených prípadoch prísne chránené,
- ktoré sú klasifikované z hľadiska **dostupnosti** klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,
- ktoré sú klasifikované z hľadiska **integrity** klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,
- pri ktorých je potrebné identifikovať zodpovednosť za kritické aktivity, najmä však aktivity privilegovaných používateľov,
- pri ktorých je potrebné vykonávať kontrolnú činnosť,
- zabezpečujúce vytváranie a vedenie agend, ktoré nepatria do I. bezpečnostnej kategórie,
- ktoré sú agendové informačné systémy,
- ktorými sú špecializované portály,
- ktoré sú nevyhnutné na rozhodovanie orgánu štátnej moci.

5.1.3 Kategória III.

Kategória III. zahŕňa informačné aktíva v pôsobnosti organizácie:

- **ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident II. a III. stupňa (podľa vyhlášky NBÚ č. 165/2018 Z. z.),**
- ktoré sú klasifikované z hľadiska **dôvernosti** ako **prísne chránené,**
- ktoré sú klasifikované z hľadiska **dostupnosti** klasifikačným stupňom vysoká,
- ktoré sú klasifikované z hľadiska **integrity** klasifikačným stupňom vysoká,
- pri ktorých je potrebné audítovať aktivity všetkých používateľov,
- prostredníctvom ktorých sa poskytuje základná služba a ktorých výpadok alebo poškodenie spôsobí poškodenie alebo znemožnenie poskytovania základnej služby,
- ktoré sú označené ako **utajované skutočnosti alebo ako tajomstvo podľa osobitých predpisov (napr. zákon č. 215/2004 Z. z.)**,
- **ktoré sú nevyhnutné a potrebné z hľadiska plnenia úloh týkajúcich sa obrany a bezpečnosti štátu alebo**,
- ktorým je ústredný portál verejnej správy

6. Určenie parametrov pre cloudovú službu

Metodické usmernenie pri určovaní parametrov C, I, A a úrovne cloudových služieb U, vychádza z definícií vyššie uvedených predpisov (viď časť 1.1 Legislatíva).

Pre jednoduchosť boli základné pravidlá prenesené do tabuliek v prílohe č. 1., ktorá obsahuje záložky a v jednotlivých krokoch je potrebné vyplniť editovateľné položky v tabuľkách umiestnených v záložkách.

Pri určovaní parametrov je potrebné venovať pozornosť a vyplniť údaje na záložkách, ktoré sú farby modrej a zelenej. Červené záložky sú pomocné, ktoré pomáhajú pri určovaní údajov.

Pre určenie správnych odpovedí môže napomôcť vopred vykonaná analýza rizík.

6.1. Popis záložiek – 0. Metodický postup

Táto záložka obsahuje metodický postup ako pristupovať k vypĺňaniu tabuliek na ďalších záložkách.

Je však potrebné vyplniť:

1. Názov ISVS, pre ktorý sa zisťujú parametre U, C, I, A.
2. ID uvedeného ISVS(kód MetaIS), ktorý musí byť evidovaný v meta-informačnom systéme verejnej správy.

V tejto záložke sa po vykonaní a správnom vyplnení údajov zobrazia výsledné hodnoty **Ux, Cx, Ix, Ax**.

6.2. Popis záložiek – 1. Dôvernosť

Záložka „1. Dôvernosť“ obsahuje tabuľku so zoznamom požiadaviek, ktoré musia byť splnené pre jednotlivé stupne ochrany informačného aktíva z pohľadu zachovania dôvernosti (bezpečnosti), to určuje klasifikačný stupeň pre „Dôvernosť“ informačného aktíva.

- Prísne chránené – C3
- Chránené – C2

- Interné – C1
- Verejné – C0

V stĺpci „E“ vyplníme hodnotu „**1**“ pre odpoveď „ÁNO“, hodnotu „**0**“ pre odpoveď „NIE“

Vyplňte odpovede pokiaľ možno len pre ten klasifikačný stupeň, ktorého požiadavky najviac zodpovedajú skutočnosti, teda požiadavkám na informačné aktíva, ktoré spracováva alebo uchováva ISVS, ktorý práve klasifikujeme z pohľadu dôvernosti. Odporúčame postupovať zhora nadol.

O celkovej hodnote klasifikačného stupňa „Dôvernosť“ rozhodujú odpovede „ÁNO(1)“ patriace k najvyššej hodnote C3 alebo C2 alebo C1 alebo C0.

6.3. Popis záložiek – 2. Integrita

Záložka „2. Integrita“ obsahuje tabuľku so zoznamom požiadaviek, ktoré musia byť splnené pre jednotlivé stupne ochrany informačného aktíva z pohľadu zachovania integrity, to určuje klasifikačný stupeň pre „Integrita“ informačného aktíva.

- Vysoká – I3
- Stredná – I2
- Nízka – I1

V stĺpci „E“ vyplňte hodnotu „1“ pre odpoveď „ÁNO“, hodnotu „0“ pre odpoveď „NIE“

Vyplňte odpovede pokiaľ možno len pre ten klasifikačný stupeň, ktorého požiadavky najviac zodpovedajú skutočnosti, teda požiadavkám na informačné aktíva, ktoré spracováva alebo uchováva ISVS, ktorý práve klasifikujete z pohľadu zachovania integrity. Odporúčame postupovať zhora nadol.

O celkovej hodnote klasifikačného stupňa „Integrita“ rozhodujú odpovede „ÁNO(1)“ patriace k najvyššej hodnote I3 alebo I2 alebo I1.

6.4. Popis záložiek – 3. Dostupnosť

Záložka „3. Dostupnosť“ obsahuje tabuľku so zoznamom požiadaviek, ktoré musia byť splnené pre jednotlivé stupne ochrany informačného aktíva z pohľadu zachovania dostupnosti. To určuje klasifikačný stupeň pre „Dostupnosť“ informačného aktíva:

- Vysoká – A3
- Stredná – A2
- Nízka – A1

V stĺpci „E“ vyplňte hodnotu „1“ pre odpoveď „ÁNO“, hodnotu „0“ pre odpoveď „NIE“

Vyplňte odpovede pokiaľ možno len pre ten klasifikačný stupeň, ktorého požiadavky najviac zodpovedajú skutočnosti, teda požiadavkám na informačné aktíva, ktoré spracováva alebo uchováva ISVS, ktorý práve klasifikujete z pohľadu zachovania dostupnosti. Odporúčame postupovať zhora nadol.

O celkovej hodnote klasifikačného stupňa „Dostupnosť“ rozhodujú odpovede „ÁNO(1)“ patriace k najvyššej hodnote A3 alebo A2 alebo A1.

6.5. Popis záložiek – 4. Kategórie systémov

V záložke „4. kategórie systémov“ sú tri tabuľky, v ktorých sa vypĺňajú len položky označené žltou farbou.
Ostatné náležitosti sa vyplnia podľa výsledkov s vypĺňania údajov v

- Popis záložiek – 1. Dôvernosť
- Popis záložiek – 2. Integrita
- Popis záložiek – 3. Dostupnosť

Presný postup je popísaný v nasledujúcej kapitole.

6.6. Určenie parametrov C, I, A a určenie parametra Ux cloudovej služby

Metodický postup:

1. Otvorte dokument – súbor – *P01_Urcenie_parametrov_UxCxIxAx.xlsx*
    a) Na záložke „0“ vyplňte názov ISVS, pre ktorý chcete určiť parametre UxCxIxAx.
2. Je potrebné urobiť analýzu vášho informačného aktíva - ISVS z pohľadu jeho dôležitosti a údajov, s ktorými ISVS pracuje, a ktoré uchováva.
   V analýze je potrebné sa zamerať na nasledujúce:
    a) je nutné urobiť analýzu údajov, s ktorými ISVS pracuje, pripadne ktoré údaje uchováva,
    b) nájsť odpovede na to, či je splnená požiadavka v záložkách 1., 2., 3.,
    c) je doporučené urobiť analýzu rizík pre informačné aktívum – ISVS.
3. V záložkách 1., 2., 3., sa nachádzajú požiadavky pre klasifikačné stupne 0,1,2,3,
    a) vyberte klasifikačnú úroveň, ktorej požiadavky najlepšie charakterizujú bezpečnosť informácií vo vašom ISVS a pre vybrané požiadavky vyplňte v stĺpci „**E**“ odpoveď „**1**“, čo znamená „**Áno**“.
    b) v ostatných položkách stĺpca „**E**“ musí byť nastavená „**0**“, čo znamená „**Nie**“.
4. Po takto vyplnených odpovediach na splnenie požiadaviek sa na záložke „0“ zobrazia určené parametre CIA.
5. Prejdite na záložku 4.
    a) Položky E5, F5, G5 obsahujú hodnoty C,I,A, ktoré sú preneseným výsledkom zo záložiek 1.,2.,3., => **Požadovaná hodnota CIA**
    b) Stĺpce O,P,Q zobrazujú možné(**Podporované**) kombinácie CIA
    c) Ak vami požadovaná hodnota CIA zodpovedá niektorej z podporovaných kombinácií, vyfarbí sa v stĺpci „**R**“ políčko označujúce zhodu **Požadovanej** hodnoty s **Podporovanou** hodnotou. Farba políčka zároveň ukazuje, v ktorej tabuľke (označené I., II., III.,) podľa stĺpca „**B**“ je potrebné zodpovedať ďalšie odpovede – stĺpec „**M**“ – **Odpoveď**, je potrebné vyplniť polia označené **žltou farbou**.
    d) **UPOZORNENIE 1!** - Môže sa stať, že sa nevyfarbí v stĺpci „R“ žiadne políčko príslušnou farbou.
    To znamená, že je potrebné sa vrátiť k záložkám 1., 2.,3., a prehodnotiť odpovede.
    V záložke v stĺpcoch O,P,Q sa nachádzajú kombinácie, ktoré majú zmysel vychádzajúci zo zákona č. 69/2018 Z. z. a vyhlášky č. 362/2018 Z. z.
    Napríklad, ak má ISVS hodnotu dôvernosti C=3, Integrita a Dostupnosť by nemala byť menšia ako 2.
    e) **UPOZORNENIE 2!** – Môže sa stať, že je potrebné vyplniť odpovede v dvoch tabuľkách. Odpovede potom bližšie špecifikujú jednoznačnejší výsledok.

*Po kompletnom vyplnení odpovedí v označených tabuľkách by nemalo zostať žiadne políčko v stĺpci „**K**" označene červenou farbou.*

f) Po zodpovedaní otázok v stĺpci „**M**" sa v položke „**M3**" bude nachádzať výsledná hodnota **Ux.**

6. Po ukončení vypĺňania potrebných položiek v záložke 4, budú výsledné hodnoty UX Cx, Ix, Ax zobrazene v záložke „**0. Metodický postup**"
7. Podľa takto získaných hodnôt následne vyhľadávate v Katalógu služieb Vládneho cloudu vhodné cloudové služby pre vaše informačné aktívum-ISVS.

7. Revízia dokumentu

Metodické usmernenie sa reviduje a aktualizuje najmenej každé dva roky.

Metodické usmernenie sa aktualizuje aj častejšie, ak:

- nastane požiadavka na jeho aktualizáciu,
- pri zásadných zmenách v organizácii a štruktúre organizácie,
- pri zásadných zmenách v legislatíve Slovenskej republiky s vplyvom na niektorú časť tohto dokumentu (príslušná relevantná legislatíva je súčasťou prílohy č. 1 Bezpečnostnej politiky kybernetickej bezpečnosti).

Za pravidelnú revíziu a aktualizáciu metodického usmernenia zodpovedá oddelenie Správy biznis, aplikačnej a technologickej architektúry Sekcie informačných technológií verejnej správy.

Metodické usmernenie a všetky následné aktualizácie schvaľuje generálny riaditeľ sekcie informačných technológií verejnej správy.

8. Prílohy

8.1. Príloha č. 1 – Dotazník slúžiaci na určenie klasifikačných stupňov

P01_Urcenie_parametrov_UxCxIxAx.xlsx

8.2. Príloha č. 2 – Príklady vykonanej klasifikácie

P01_Urcenie_parametrov_UxCxIxAx-ITAM .xlsx

P01_Urcenie_parametrov_UxCxIxAx-MetaIS.xlsx