Správa o výsledku kontroly informačných systémov v Trenčianskom samosprávnom kraji a vo vybranej organizácii v jeho zriaďovateľskej pôsobnosti

Úvod

Kontrola informačných systémov bola vykonaná nad rámec plánu kontrolnej činnosti Najvyššieho kontrolného úradu Slovenskej republiky (ďalej len „NKÚ SR“) na rok 2008, v intenciách projektu realizovaného s finančnou podporou Európskej únie v rámci programu Prechodný fond.

Účelom kontrolnej akcie bolo preverenie informačných systémov (ďalej len „IS“), ich bezpečnosť, spoľahlivosť a korektnosť. Preverenie údajov v týchto systémoch so zreteľom na spoľahlivosť, úplnosť a dostatočnosť ich zabezpečenia. Kontrolná akcia bola vykonaná podľa Európskej vykonávacej smernice pre kontrolné štandardy INTOSAI formou všeobecnej kontroly IS a pri vybraných aplikáciách bola použitá aplikačná kontrola IS.

Predmetom kontroly boli oblasti:

1. Prevádzka IS
2. Bezpečnosť IS
3. Operačné systémy a siete
4. Aplikačná kontrola

Kontrola bola vykonaná v termíne od 28.10.2008 do 25.11.2008 v subjektoch:

- Trenčiansky samosprávny kraj, Predmetom kontroly boli oblasti 1 – 3.
- Správa ciest Trenčianskeho samosprávneho kraja, Predmetom kontroly bola oblasť 4.

Kontrola bola vykonaná za obdobie roku 2008.

Výsledky kontroly

1. Prevádzka IS

V podmienkach Trenčianskeho samosprávneho kraja (ďalej len „TSK“) je správa a riadenie informačných technológií (ďalej len „IT“) a IS v kompetencii oddelenia informatiky, ktoré je organizačne začlenené pod úsek riaditeľa Úradu Trenčianskeho samosprávneho kraja. TSK poveril budovaním a prevádzkou komplexného IS TSK externého poskytovateľa tejto služby na základe zmluvy o systémovej integrácii a nadštandardnom servise.

Kontrolou boli zistené viaceré nedostatky týkajúce sa oblasti organizácie a riadenia činností

v rámci oddelenia informatiky TSK.

Nezabezpečený dohľad a proces schvaľovania v rámci oddelenia informatiky môže viesť k neoprávneným a nesprávnym rozhodnutiam, ktoré nebudú korešpondovať so stanovenými cieľmi organizácie.

V zmysle § 3 zákona NR SR č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o ISVS“) je TSK ako správca IS verejnej správy povinnou osobou, ktorá je povinná zabezpečiť, aby IS verejnej správy vyhovoval štandardom ustanoveným vo Výnose Ministerstva financií Slovenskej republiky č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos o štandardoch pre ISVS“).

Vykonanou kontrolou bol zistený nesúlad s bezpečnostnými štandardami výnosu o štandardoch pre ISVS v oblastiach kontrolného mechanizmu riadenia informačnej bezpečnosti, periodického hodnotenia zraniteľnosti, zálohovania a v oblasti fyzického ukladania záloh.

Zistený nesúlad s platnými ustanoveniami výnosu o štandardoch pre ISVS je v rozpore s § 3 zákona o ISVS, v ktorom je stanovená povinnosť správcu IS verejnej správy zabezpečiť, aby IS verejnej správy vyhovoval štandardom.

Ďalej boli zistené nedostatky v oblasti dodržiavania zásad a postupov bezpečnosti IT upravené v bezpečnostnej politike kontrolovaného subjektu a taktiež boli zistené nedostatky v oblasti nepretržitej prevádzky a obnovy systému.

Nezabezpečenie zásad nepretržitej prevádzky a obnovy systému môže viesť k strate a poškodeniu údajov a k prípadnému znefunkčneniu prevádzky IS nad prípustný časový limit.

2. Bezpečnosť IS

Kontrolou bezpečnosti IS TSK boli zistené viaceré nedostatky v oblasti logického prístupu do IS a taktiež bolo zistené nevhodné nastavenie systémového zaznamenávania vykonaných operácií v ekonomickom IS (ďalej len „EIS“) kontrolovaného subjektu. Na základe upozornenia kontrolnej skupiny sa čiastočná náprava uvedeného stavu uskutočnila počas výkonu kontroly.

Nevhodná bezpečnostná politika môže mať za následok získanie neautorizovaného prístupu do IS a k údajom v tomto IS, čím vzniká riziko úniku, neautorizovanej zmeny, straty, odcudzenia ale i možného zneužitia údajov v takomto IS.

V oblasti prístupu tretích strán subjekt využíva externých poskytovateľov služieb v oblasti systémovej integrácie a nadštandardnom servise a v oblasti implementácie a správy EIS. Tieto činnosti sú vykonávané na zmluvnom základe.

Kontrolou bolo zistené nedostatočné vymedzenie služieb poskytovaných tretími stranami v oblasti správy komplexného IS TSK a taktiež správy EIS. Ďalej bolo kontrolou zistené, že nie je stanovený presný rozsah prístupu tretích strán do produkčného prostredia EIS implementovaného na TSK.

Nepresné vymedzenie zmluvne dohodnutých služieb môže mať nepriaznivý vplyv na rozsah a kvalitu vykonávaných činností pre príjemcu týchto služieb. Existuje riziko, že finančné prostriedky objednávateľa služby nebudú vynakladané hospodárne, efektívne a účinne.

Preverením oblasti fyzickej bezpečnosti bolo zistené, že technické miestnosti s kľúčovými

Preverením oblasti fyzickej bezpečnosti bolo zistené, že technické miestnosti s kľúčovými aktívami IT kontrolovaného subjektu nevyhovujú medzinárodným štandardom pre fyzickú bezpečnosť.

V dôsledku nevhodného fyzického zabezpečenia môže dôjsť k významnému ohrozeniu aktív IS organizácie - či už vo forme odcudzenia hardvéru alebo údajov v IS - alebo aj k ich možnému zničeniu spôsobenému nepredvídanou udalosťou.

3. Operačné systémy a siete

Údržba operačných systémov a aplikácií je vykonávaná v rámci poskytovaných služieb externým poskytovateľom na základe zmluvy o nadštandardnom servise. Na základe tejto zmluvy sa taktiež vykonáva monitorovanie hardvérového vybavenia IT.

Preverením systému údržby operačných systémov a aplikačného vybavenia v rámci IS bolo zistené, že kontrolovaný subjekt nemá dostatočne zavedený proces implementácie aktualizácií operačných systémov a aplikačného vybavenia, čo môže viesť k nežiaducim stavom dostupnosti jednotlivých aplikácií a údajov v IS.

V oblasti správy údajov, databáz a užívateľských účtov bolo zistené, že nastavená politika užívateľských hesiel nezodpovedá bežným bezpečnostným štandardom.

Nedodržanie bezpečnostných pravidiel politiky hesiel môže viesť k neoprávnenému vniknutiu do IS TSK, v dôsledku čoho môže dôjsť k neoprávnenej zmene prípadne k odcudzeniu údajov z IS.

4. Aplikačná kontrola

Aplikačná kontrola bola vykonaná v subjekte Správa ciest Trenčianskeho samosprávneho kraja (ďalej len „SC TSK“), ktorého zriaďovateľom je TSK, kde bol kontrolovaný EIS využívaný SC TSK.

Na kontrolovanom subjekte SC TSK sú implementované jednotlivé moduly EIS a ich komponenty pre spracovanie ekonomických činností, logistiky, evidencie majetku a sumarizácie údajov pre potreby Úradu TSK. Technologické riešenie EIS je založené na dvojvrstvovej architektúre klient/server.

Správu EIS vykonáva oddelenie informatiky Úradu TSK. Kontrolou bolo zistené, že nie sú dostatočne vymedzené povinnosti poskytovateľa EIS v oblasti administrácie aplikácie a taktiež, že nie sú formálne stanovené zodpovednosti jednotlivých oddelení za vstupy a spracovanie výstupov v EIS.

Nezabezpečením formálne určenej zodpovednosti za vstupy a za spracovanie výstupov vzniká riziko nesprávnych údajov v EIS a ich výstupov bez možnosti určenia konkrétnej zodpovednosti.

Vykonaná kontrola preukázala, že vnútorné kontroly zamerané na vstup, prenos a výstup údajov v EIS poskytujú dostatočnú istotu, že údaje a výstupy z tohto systému sú spoľahlivé, úplné a dostatočne zabezpečené.

Záver

Kontrolou bolo zistené porušenie všeobecne záväzného právneho predpisu v dôsledku čoho bolo odporučené prijať nasledovné opatrenia.

V oblasti prevádzky IS:

V rámci oddelenia informatiky v každej funkčnej oblasti vymedziť adekvátne úrovne

- V rámci oddelenia informatiky v každej funkčnej oblasti vymedziť adekvátne úrovne dohľadu a procesu schvaľovania prostredníctvom smernice upravujúcej schvaľovací proces.
- Vypracovať a každoročne prehodnocovať strategické plány IT, ktoré musia byť schválené vedúcimi pracovníkmi. Vypracovať politiku riadenia zmien, ktorá riadi vývoj a rozširovanieaplikácií a zabezpečuje, aby boli nové programy v plnom rozsahu testované a prijaté užívateľom.
- Zabezpečiť súlad s platnou legislatívou v oblasti IS a komunikačných technológií. Zabezpečiť, aby IS bol v súlade s výnosom o štandardoch pre ISVS. Vymenovať bezpečnostného pracovníka, ktorý okrem iného periodicky vypracováva formálne správy o stave bezpečnostných postupov a tieto správy predkladá vedeniu. Ďalej bolo odporučené vykonávať pravidelné kontroly a školenia zamestnancov v oblasti bezpečnosti IS a vyžadovať dodržiavanie zásad bezpečnosti a ostatných prevádzkových predpisov, vrátane dodržiavania pravidiel fyzického zabezpečenia.
- V oblasti zásad nepretržitej prevádzky a obnovy systému bolo odporučené zaviesť podrobné zásady a postupy týkajúce sa zálohovania údajov a programov a naplánovať ich ako súčasť bežných denných činností. V primeraných časových intervaloch vytvárať záložné kópie hlavných kľúčových súborov, operačných systémov, kľúčových aplikácií a dokumentácie k nim a tieto uchovávať mimo miesta prevádzky.
- Prijať plán pre prípad nepredvídaných okolností, zaviesť postupy obnovy a reštartovania, vrátane rýchlej obnovy poškodených alebo stratených súborov a pravidelne ich testovať. Kópie plánu pre prípad nepredvídaných okolností uchovávať na vzdialenom mieste.

V oblasti bezpečnosti IS:

- Zaviesť a dôsledne uplatňovať bezpečnostnú politiku v rámci organizácie i vo vzťahu k tretím osobám. Zabezpečiť fyzickú bezpečnosť a bezpečnosť prostredia v súlade so štandardami pre fyzickú bezpečnosť.
- Spresniť rozsah dohodnutých služieb v servisnej zmluve pre EIS, presnú definíciu poskytovaných služieb, ich kvalitu a periodicitu vykonávania, stanovenie konkrétnych výstupov za jednotlivé činnosti.
- Zabezpečiť archiváciu systémových údajov EIS na vzdialenom mieste.
- Vyžadovať od tretích strán pravidelné správy o prístupe do produkčného prostredia EIS a vykonaných činnostiach v tomto systéme.
- Spresniť rozsah dohodnutých služieb a stanoviť konkrétne výstupy za jednotlivé činnosti, ktoré poskytuje externý poskytovateľ na základe zmluvy o nadštandardnom servise. Pravidelne posudzovať kvalitu vykonávaných služieb.

V oblasti operačných systémov a sietí:

- Prijať zásady schvaľovania a implementácie aktualizácií operačných systémov a aplikačného vybavenia.
- Prijať takú bezpečnostnú politiku prístupu do IS, ktorá bude v súlade so všeobecne uznávanými zásadami bezpečnosti a ktorá minimalizuje riziko neoprávneného vstupu do IS. Formálne stanoviť systém prideľovania a schvaľovania užívateľských účtov a účtov elektronickej pošty.

V oblasti správy EIS na základe aplikačnej kontroly bolo odporučené:

- Presne vymedziť povinnosti externého poskytovateľa aplikácie v oblasti jej administrácie.
- Formálne stanoviť zodpovednosti jednotlivých oddelení resp. zamestnancov za vstupy a spracovanie výstupov v IS.

Aplikačná kontrola EIS preukázala, že vnútorné kontroly zamerané na vstup, prenos a výstup údajov v EIS poskytujú dostatočnú istotu, že údaje a výstupy z tohto systému sú spoľahlivé, úplné a dostatočne zabezpečené.

Výsledky vykonanej kontroly boli prerokované so štatutárnymi zástupcami kontrolovaných subjektov, ktorí prijali 8 opatrení na odstránenie kontrolou zistených nedostatkov. Plnenie prijatých opatrení bude NKÚ SR v rámci svojej činnosti sledovať a kontrolovať.