Valstybinio audito ataskaita santrauka

YPATINGOS SVARBOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMAS

2018 m. birželio 28 d. Nr. VA-2018-P-900-3-6

Su valstybinio audito ataskaita galima susipažinti
Valstybės kontrolės interneto svetainėje www.vkontrole.lt

SANTRAUKA

Audito svarba

Valstybės informaciniai ištekliai yra informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma[1]. Ypatingos svarbos valstybės informaciniai ištekliai – ypatingos svarbos elektroninė informacija – tvarkomi pirmos kategorijos valstybės informacinėse sistemose, registruose ir kadastruose (toliau – IS). Šių sistemų pagalba įgyvendinamos svarbios valstybės funkcijos, pvz., valstybės finansų valdymas, mokesčių administravimas, sveikatos apsauga. Ypatingos svarbos informacijos praradimas ir IS, kurios tvarko šią informaciją, nepasiekiamumas gali turėti skaudžių pasekmių visuomenės saugumui ir gerovei bei ekonomikai.

Tinkamai sukurti ir efektyviai įgyvendinami informacinių technologijų procesai sudaro sąlygas veiksmingai apsaugoti informacinius išteklius nuo kylančių kibernetinių grėsmių. Pastaraisiais metais pasaulyje kibernetinių atakų taikiniu vis dažniau tampa ypatingos svarbos informaciniai ištekliai, kuriais teikiamos visuomenei svarbios paslaugos ir kuriuose saugoma ypač svarbi informacija. 2018 m. pasaulinių rizikų ataskaitoje nurodoma, kad ateityje šių atakų tikimybė augs, kartu augs pavojus sutrikdyti ypatingos svarbos informacinių išteklių darbą[2]. Nacionalinio kibernetinio saugumo centro duomenimis, kibernetinių incidentų Lietuvoje skaičius 2017 m. sudarė 54,4 tūkst. ir, palyginus su 2016 m., jų užregistruota dešimtadaliu daugiau[3]. Todėl, didėjant kibernetinių grėsmių lygiui, labai svarbu stiprinti ypatingos svarbos valstybės informacinių išteklių saugumą. Pasaulio kibernetinio saugumo indekso[4] 2017 m. rezultatais, Lietuva pasaulyje buvo 57-oje vietoje iš 165 šalių, o iš ES šalių – 23-ioje. Tai rodo, kad saugumo valdymo efektyvumas yra didintinas.

Aukščiausiosios audito institucijos 2006–2016 m. laikotarpiu atlikti informacinių technologijų bendrosios kontrolės vertinimai parodė besikartojančias IT valdymo sričių (planavimo, informacijos architektūros apibrėžimo, organizacinės struktūros, pokyčių, veiklos tęstinumo užtikrinimo, duomenų saugos, IT valdymo stebėsenos ir vertinimo) problemas. Audituotų viešojo sektoriaus subjektų IT valdymo branda per paskutinius dešimt metų vidutiniškai siekė pirmąjį brandos lygį iš 5-ių[5] ir šuo metu fiksuojame 1,7 brandos lygį. Žemas ypatingos svarbos valstybės informacinių išteklių brandos lygis rodo valstybės informacinių išteklių politikos formavimo ir įgyvendinimo trūkumus, o tai sudaro sąlygas didesniam šių išteklių pažeidžiamumui.

[1] LR valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 2 str. 17 p.

[2] Pasaulio ekonomikos forumo pasaulinių rizikų ataskaita (angl. *Insight Report „The Global Risks Report 2018" by the World Economic Forum*). Prieiga per internetą: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[3] Prieiga per internetą: https://www.nksc.lt/.

[4] Pasaulinis kibernetinio saugumo indeksas *(angl.* Global Cyber Security Index, GCI), prieiga per internetą: https://www.itu.int/pub/D-STR-GCI.01-2017. Indeksas matuoja kibernetinio atsparumo galimybes 195 pasaulio valstybėse ir leidžia palyginti valstybių kibernetinio saugumo būklę.

[5] Pagal COBIT metodiką.

Aukščiausioji audito institucija nusprendė atlikti ypatingos svarbos valstybės informacinių išteklių auditą: įvertinti šių išteklių valdymo ir saugumo būklę ir numatyti priemones, kaip ją gerinti.

Audito tikslas ir apimtis

Tikslas – įvertinti ypatingos svarbos valstybės informacinių išteklių valdymą (bendrąją kontrolę), brandą ir nustatyti sistemines valstybės informacinių išteklių valdymo problemas.
Audito subjektai:

- Susisiekimo ministerija formuoja valstybės informacinių išteklių plėtros politiką. Audito metu Vyriausybė 2018-06-20 posėdyje priėmė sprendimą pritarti įstatymų pakeitimams, kuriais valstybės informacinių išteklių plėtros politikos, kai kurios registrų politikos ir informacinės visuomenės plėtros politikos formavimo ir koordinavimo funkcijos bus priskirtos Ūkio ministerijos kompetencijai[6];
- Vidaus reikalų ministerija iki 2018-01-01 formavo politiką valstybės informacinių išteklių saugos srityje;
- Krašto apsaugos ministerija formuoja kibernetinio saugumo politiką, organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą, nuo 2018-01-01 formuoja politiką valstybės informacinių išteklių saugos srityje;
- Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos atsako už valstybės informacinių išteklių funkcinį suderinamumą, kūrimą, tvarkymą ir plėtrą.

IT valdymo brandą vertinome 12-oje viešojo sektoriaus organizacijų[7], kurios tvarko 44-ias pirmos kategorijos IS, iš jų 10-yje atlikome detalią atrinktų IT valdymo procesų analizę. Dvi organizacijos nevertintos, nes vienos, atlikus pirminį vertinimą, branda siekė 0 lygį, kitoje po 2016 m. aukščiausios audito institucijos atlikto IT bendrosios kontrolės audito neįvyko pokyčių.

Atlikę visų 34-ių COBIT procesų išankstinį vertinimą, detalius vertinimus atlikome šiose rizikingiausiose srityse:

- IT strateginis planavimas;
- Informacinės architektūros nustatymas;
- IT rizikų valdymas;
- Pokyčių valdymas;
- Nepertraukiamo paslaugų teikimo užtikrinimas;
- Sistemų saugumo užtikrinimas;
- Duomenų tvarkymas;
- IT veiklos stebėsena ir vertinimas;
- IT valdymo užtikrinimas.

Procesų vertinimas apėmė ir organizacijos, ir nacionalinį IT valdymą, šių valdymo lygių abipusę sąveiką. Informacinių išteklių valdymą ir brandą vertinome pagal 2017 m. būklę. Analizuodami tam tikrų procesų nuoseklumą ir tęstinumą, naudojome 2014–2017 m. duomenis.

[6] LR Vyriausybės posėdžio 2018-06-20 protokolas Nr. 27, 7 kl., Lietuvos Respublikos Vyriausybės kanceliarijos Politikos įgyvendinimo grupės 2018-06-20 pažyma Nr. NV-1585.
[7] Valstybinė mokesčių inspekcija, VĮ Registrų centras, Informatikos ir ryšių departamentas, Valstybinio socialinio draudimo fondo valdyba, VĮ Žemės ūkio informacijos ir kaimo verslo centras, Muitinės informacinių sistemų centras, Valstybinė maisto ir veterinarijos tarnyba, LR Seimo kanceliarija, Finansų ministerija, Informacinės visuomenės plėtros komitetas, Valstybinė ligonių kasa, Valstybinė miškų tarnyba.

Auditas atliktas pagal Valstybinio audito reikalavimus ir tarptautinius aukščiausiųjų audito institucijų standartus. Vertinimas atliktas pagal COBIT[8] metodiką ir atitiktį Lietuvos Respublikos teisės aktų reikalavimams ir rekomendacijoms dėl valstybės informacinių išteklių valdymo. Ypatingos svarbos valstybės informacinių išteklių valdymo vertinimas atliktas vadovaujantis Informacinių technologijų audito vadovu[9], 5300-uoju tarptautiniu aukščiausiųjų audito institucijų standartu, Informacinių sistemų audito ir kontrolės asociacijos (ISACA) tarptautiniais audito standartais, atsižvelgta į ISACA audito gaires ir gerąją praktiką.

Audito apimtis ir taikyti metodai išsamiau aprašyti 2 priede „Audito apimtis ir metodai“ (38 psl.). Atlikdami auditą darėme prielaidą, kad visi auditoriams pateikti dokumentai yra teisingi, išsamūs ir galutiniai, o jų kopijos atitinka originalus.

Išvados

Ypatingos svarbos valstybės informacinių išteklių valdymo brandos pokyčių tendencijos yra teigiamos, tačiau stebima pažanga, atsižvelgus į didėjantį kibernetinių grėsmių lygį, yra per lėta, ir šių išteklių saugumas turi būti užtikrinamas labiau. Tai lemia šie trūkumai:

1. Ypatingos svarbos valstybės informacinių išteklių nustatymo sistema yra nepakankamai veiksminga, kad būtų įgyvendinami saugumo sprendimai, atitinkantys realius poreikius:
    1.1. vertinimams, kurie pagrįstų valstybės informacinių išteklių ypatingą svarbą, trūksta objektyvumo, esant pokyčiams ne visada atliekami pakartotiniai vertinimai, šis procesas neprižiūrimas šalies mastu, o svarbos nustatymo gairės neužtikrino efektyvaus jo įgyvendinimo (1.1 poskyris, 12 psl.);
    1.2. ypatingos svarbos valstybės informacinių išteklių bei ypatingos svarbos informacinės infrastruktūros identifikavimo sistema nėra bendra, jie identifikuojami skirtingais būdais pagal informacijos ir paslaugų svarbą, o tai apsunkina šių išteklių nustatymo procesą (1.2 poskyris, 15 psl.);
    1.3. nėra sukurta nacionalinė informacinė architektūra, kuri atvaizduotų valstybės IS, jų tarpusavio ryšius, parodytų ypatingos svarbos valstybės informacinių išteklių mastą ir suteiktų galimybę priimti pagrįstus sprendimus dėl šių išteklių svarbos (1.2 poskyris, 15 psl.).
2. Valstybės informacinių išteklių valdymas turėtų labiau atitikti gerąsias IT valdymo praktikas ir standartus tam, kad vyktų kompleksinis IT srities tobulinimas, galintis prisidėti prie didesnės ypatingos svarbos valstybės informacinių išteklių valdymo pažangos:
    2.1. IT planavimas nėra darnus: planuojamos įgyvendinti IT priemonės pateikiamos skirtinguose dokumentuose, dėl strateginių dokumentų gausos trūksta sisteminio požiūrio, todėl sudėtinga nustatyti svarbiausius prioritetus ir nukreipti išteklius didžiausioms grėsmėms valdyti. Esant tokiai sistemai, IT plėtros planai ne visais atvejais parengiami, o parengtieji nėra išsamūs, nerengiami detalūs įgyvendinimo priemonių planai (2.1 poskyris, 17 psl.);

[8] COBIT (*Control Objectives for Information and related Technologies*) – tarptautinės ISACA organizacijos standartas, aprašantis geriausią IT valdymo praktiką.
[9] Patvirtintas LR valstybės kontrolieriaus 2017-06-21 įsakymu Nr. V-165.

2.2. IT stebėsena neužtikrina, kad organizacijose būtų matuojamas IT veiklos efektyvumas, o YSVII tvarkytojų atliekami auditai parodytų tikrą IT valdymo brandą. Šalies mastu nestebima faktinė IT valdymo būklė, sistemiškai neanalizuojama IT valdymo problematika. Sukurta Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema, skirta tik saugos atitikties stebėsenai palengvinti, tačiau jos funkcionalumas nėra pakankamai panaudojamas (2.2 poskyris, 19 psl.).

3. Nepakankamai veiksmingai įgyvendinamos priemonės, galinčios užtikrinti ypatingos svarbos informacinių išteklių atsparumą kibernetinių grėsmių lygiui, todėl šių išteklių pažeidžiamumo rizika išlieka:

   3.1. IT saugumo rizikų vertinimo veiksmingumas turėtų būti didinamas – identifikuojamos ne visos aktualios rizikos, o jų vertinimo metodika neatitinka naujausių IT valdymo praktikų, neužtikrinamas nepriimtinų rizikų valdymas laiku (3.1 poskyris, 23 psl.);

   3.2. sistemiškai nėra naudojamos organizacinės saugumo priemonės, galinčios sumažinti kibernetines grėsmes: IS kūrimo, modernizavimo, modifikavimo metu nepakankamai testuojamas saugumas, nepakankamai ugdomas personalas; nevaldoma programinės įrangos saugi konfigūracija ir atnaujinimai, IT veiklos tęstinumo ir atsarginių kopijų netinkamas valdymas kelia grėsmę veiklos atkūrimui, saugos veiksmingumo matavimai nėra pakankami ir neprisideda prie saugumo didinimo (3.2 poskyris, 26 psl.).

Rekomendacijos

Lietuvos Respublikos Vyriausybei

Siekiant užtikrinti geresnę valstybės informacinių išteklių valdymo kokybę ir aukštesnę YSVII tvarkytojų IT valdymo brandą, reikėtų:

1. Sukurti nacionalinę informacinę architektūrą ir jos valdymo mechanizmą, kuris leistų objektyviai nustatyti valstybės informacinių išteklių svarbą bei tinkamai kontroliuoti šį procesą ir suderinti ypatingos svarbos valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros nustatymo mechanizmus.
2. Išvystyti IT gerąsias valdymo praktikas atitinkantį valstybės informacinių išteklių valdymo mechanizmą, kuris užtikrintų bendrą ir į svarbiausius prioritetus orientuotą planavimą, numatytų siektiną IT valdymo brandos lygį ir pažangą vertinti leidžiantį stebėsenos mechanizmą, efektyviai naudojant sukurtas technines priemones.

Krašto apsaugos ministerijai

Siekiant užtikrinti ypatingos svarbos valstybės informacinių išteklių saugumą ir atsparumą didėjančioms kibernetinėms grėsmėms, reikia:

3. Gerinti kibernetinio saugumo rizikų valdymą: atnaujinti reikalavimus, metodikas, ir diegti nacionalinį IT rizikų valdymą, leidžiantį veiksmingai valdyti šalies mastu aktualias rizikas.

4. Didinti kibernetinio saugumo valdymo organizavimo ir įgyvendinimo efektyvumą: sukurti reikiamus kontrolės mechanizmus, kurie prisidėtų prie žmogiškųjų išteklių saugumo žinių ir gebėjimų didinimo, saugumo reikalavimų įgyvendinimo būklės gerėjimo ir IS pažeidžiamumų prevencijos.

Rekomendacijų įgyvendinimo priemonės ir terminai pateikti ataskaitos dalyje „Rekomendacijų įgyvendinimo planas“ (33 psl.). Informacija apie ypatingos svarbos valstybės informacinių išteklių tvarkytojų IT brandos lygį buvo pateikta atskirais raštais.