VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

SAUGUMO PRIEMONIŲ (PRIEIGŲ VALDYMO, INFORMACIJOS, PROGRAMINĖS ĮRANGOS IR INFORMACINIŲ SISTEMŲ ATSARGINIŲ KOPIJŲ, ĮVYKIŲ ŽURNALINIŲ ĮRAŠŲ) STEBĖSENOS APIBENDRINIMAS

Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija), vadovaudamasi Valstybinės duomenų apsaugos inspekcijos 2025 metų planinių patikrinimų ir stebėsenos planu[1], rašytinės apklausos būdu, atliko 10 sveikatos priežiūros įstaigų (toliau – Įstaiga) saugumo priemonių (prieigų valdymo, informacijos, programinės įrangos ir informacinių sistemų atsarginių kopijų, įvykių žurnalinių įrašų) stebėseną. Stebėsenos buvo atliekamos naudojant patvirtintą kontrolinį klausimyną[2].

Inspekcija, apibendrinusi atliktų stebėsenų rezultatus, išskyrė toliau pateiktus dažniausiai nustatytus su saugumo priemonėmis susijusius 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas (toliau – BDAR)) neatitikimus reglamento reikalavimams.

Kadangi Įstaigos tvarko specialių kategorijų asmens duomenis (sveikatos duomenis), vertinant įgyvendinamas organizacines ir technines saugumo priemones, turi būti atsižvelgiama į duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus bei riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms, kad būtų užtikrintas pavojų atitinkančio lygio saugumas.

Prieigos teisės

1. Stebėsenų metu patikrinta, ar Įstaigos įgyvendino prieigos teisių kontrolę prie informacinių sistemų (toliau – IS) ir procesų, susijusių su Įstaigoje tvarkomais asmens duomenimis. BDAR 5 straipsnio 1 dalies f punkte reglamentuota, kad asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas). Tvarkomų asmens

[1] Valstybinės duomenų apsaugos inspekcijos 2025 metų planinių patikrinimų ir stebėsenos planas, patvirtintas Valstybinės duomenų apsaugos inspekcijos direktoriaus 2025-02-26 įsakymu Nr. 1T-31 (1.12.E) „Dėl Valstybinės duomenų apsaugos inspekcijos 2025 metų planinių patikrinimų ir stebėsenos plano patvirtinimo“

[2] Kontrolinis klausimynas, skirtas saugumo priemonių (prieigų valdymo, informacijos, programinės įrangos ir informacinių sistemų atsarginių kopijų, įvykių žurnalinių įrašų) stebėsenai, patvirtinto Valstybinės duomenų apsaugos inspekcijos direktoriaus pavaduotojos 2025 m. kovo 5 d. įsakymu Nr. 1T-35 (1.12.E) „Dėl kontrolinio klausimyno, skirto saugumo priemonių (prieigų valdymo, informacijos, programinės įrangos ir informacinių sistemų atsarginių kopijų, įvykių žurnalinių įrašų) stebėsenai, patvirtinimo“

duomenų saugumo priemonių ir rizikos įvertinimo gairių duomenų valdytojams ir duomenų tvarkytojams[3] (toliau – Gairės) 13–20 punktuose pateiktos nuostatos yra skirtos prieigos valdymui. Privilegijuotųjų prieigos teisių naudotojams yra taikomi tie patys baziniai principai, tačiau jie papildomi griežtesniais reikalavimais, kad būtų užtikrinta maksimali duomenų apsauga (pvz.: dokumentuota, kam ir kada suteikiama privilegijuota prieiga; privilegijuotų teisių naudojimas turi būti nuolat stebimas, o veiklos žurnalai peržiūrimi; mažinamas privilegijuotųjų prieigos teisių naudotojų skaičius – privilegijuotų naudotojų turėtų būti tik tiek, kiek būtina).

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl tvarkomų asmens duomenų, daro išvadą, kad Įstaigos įgyvendino privilegijuotųjų prieigos teisių kontrolę prie IS ir procesų.

2. Stebėsenų atlikimo metu nustatyta, kad 89 proc. Įstaigų IS naudotojų prieigos teisių suteikimas yra dokumentuotas. Gairių 15 punkte pateiktos nuostatos yra skirtos prieigos valdymo politikai. Gairėse nurodyta, kad prieigos valdymo politika turi būti išsami ir dokumentuota. Organizacija šiame dokumente turi nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis.

Gerosios praktikos, susijusios su prieigos teisių suteikimo dokumentavimu, apima aiškios ir išsamios prieigos valdymo politikos parengimą, kurioje nustatomos taisyklės, teisės ir apribojimai pagal naudotojų pareigas. Kiekvienas prieigos teisių suteikimas turi būti dokumentuotas, įskaitant suteikimo pagrindimą. Rekomenduojama dokumentuoti prieigos suteikimo procedūras, apibrėžti naudotojų vaidmenis ir susijusias prieigos teises bei pildyti registrus, kuriuose fiksuojama, kas, kada ir kokias teises gavo.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS naudotojų prieigos teisių suteikimo, daro išvadą, kad daugumoje (89 proc.) Įstaigų prieigos teisių suteikimas yra dokumentuotas.

3. Stebėsenų atlikimo metu nustatyta, kad Įstaigų prieigos teisės nėra bendrinamos ir yra priskirtos tik individualiems naudotojams. Gairių 18 punkte pateiktos nuostatos yra skirtos prieigos teisių valdymui. Gairėse nurodyta, kad prieigos teisės turi būti suteikiamos / keičiamos pagal veiklos reikalavimus (vaidmenis) ir prieigos valdymo taisykles bei gavus vadovybės leidimą / patvirtinimą būtų aktyvuojamos tik sėkmingai atlikus visas procedūras. Prieigos teisės turi būti panaikinamos, kai nebereikia prieigos (pasikeitė veikla, pareigos) prie asmens duomenų. Ypač svarbu, kad organizacija nedelsdama panaikintų prieigos teises naudotojams, kurie nutraukė darbo / sutartinius santykius su organizacija (laikas, pvz., ne vėliau kaip paskutinę darbo / sutartinių santykių dieną, turi būti numatytas prieigos valdymo politikoje).

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS tvarkomų asmens duomenų, daro išvadą, kad daugumoje (89 proc.) Įstaigų prieigos teisės nėra bendrinamos ir yra priskirtos tik individualiems naudotojams.

[3] https://vdai.lrv.lt/public/canonical/1725443426/586/VDAI_saugumo_priemoniu_gaires-2024-08-19.pdf

4. Stebėsenų atlikimo metu nustatyta, kad tik 11 proc. Įstaigų prieigos teisėms užtikrinti taiko kelių veiksnių autentifikaciją (angl. MFA). Gairių 91 punkte pateiktos nuostatos yra skirtos privilegijuotiems prieigos teisių naudotojams. Gairėse nurodyta, kad privilegijuotų naudotojų (pvz., sistemų administratorių) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas kelių veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė, virtualus privatus tinklas (angl. VPN) ir kiti atitinkami saugumo mechanizmai. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.

Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimu Nr. 945 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“[4] patvirtintame Kibernetinio saugumo reikalavimų aprašo (toliau – Aprašas) XII skirsnyje „Prieigos valdymas ir kelių veiksnių tapatumo nustatymo priemonės“ nurodyta, kad naudotojas ir administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių tapatumo nustatymo priemonės (angl. MFA). Inspekcija atkreipia Įstaigų dėmesį, kad ISO standarto[5] (toliau – ISO standartas) 8.5 papunktyje „Saugus autentiškumo patvirtinimas“ nurodyta, kad autentiškumo patvirtinimo informaciją turėtų papildyti autentiškumo patvirtinimo faktoriai, skirti prieigai prie ypatingos svarbos informacinių sistemų kelių veiksnių autentifikacijos (angl. MFA) patvirtinimu. Naudojant kelių autentiškumo patvirtinimo faktorių sumažėja neleistinos prieigos galimybės.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS tvarkomų asmens duomenų, daro išvadą, kad dauguma Įstaigų (89 proc.) neįgyvendino kelių veiksnių autentifikacijos (angl. MFA) prieigos teises turintiems naudotojams.

5. Stebėsenų atlikimo metu nustatyta, kad 89 proc. Įstaigų turi nustatytas taisykles, kurios riboja bendrinių naudotojų identifikatorių (pvz., *Root*) naudojimą, įvertinus sistemų konfigūracijos galimybes. Gairių 112 punkte pateiktos nuostatos yra skirtos privilegijuotiems prieigos teisių naudotojams, turintiems operacinių sistemų administratoriaus (angl. *Root*) teises, atskirti perteklinių funkcijų vykdymą. Gairėse nurodyta, kad duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos privilegijomis.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS tvarkomų asmens duomenų, daro išvadą, kad dauguma (89 proc.) Įstaigų riboja bendrinių naudotojų identifikatorių (pvz., angl. *Root*) naudojimą.

6. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų įvykių žurnaluose registruoja visus veiksmus, kuriuos atlieka IS prieigas turintys naudotojai. Gairių 119–120 punktuose pateiktos nuostatos yra skirtos privilegijuotųjų prieigos teisių naudotojų veiksmams registruoti. Gairėse nurodyta, kad visi

[4] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

[5] ISO/IEC 27002:2022 standarto „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ (toliau – ISO standartas).

sistemų administratorių veiksmai (taip pat ir jų atliekamas naudotojų teisių papildymas, panaikinimas, keitimas) turi būti registruojami. Turi būti neįmanoma ištrinti ar pakeisti techninių žurnalinių įrašų turinio. Prieiga prie žurnalinių įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS tvarkomų asmens duomenų, daro išvadą, kad 100 proc. Įstaigų įvykių žurnaliniuose įrašuose registruoja visus veiksmus, kuriuos atlieka visi prieigas turintys naudotojai.

Atsarginės kopijos

1. Stebėsenų atlikimo metu nustatyta, kad 89 proc. Įstaigų įdiegta išsami ir dokumentais pagrįsta atsarginių kopijų (dalinių / pilnų) kūrimo ir atkūrimo politika. Gairių 131 punkte pateiktos nuostatos yra skirtos atsarginių kopijų ir duomenų atstatymo procedūrų valdymui. Gairėse nurodyta, kad atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis. ISO standarto 5.1 papunktyje „Informacijos saugumo politika“ nurodyta, kad organizacija turėtų nustatyti informacijos saugumo politiką, kad būtų galima toliau įgyvendinti informacijos saugumo kontrolės priemones – atsargines kopijas. O ISO standarto 8.13 papunktyje „Informacijos atsarginės kopijos“ nurodyta, kad sistemų atsarginės kopijos turėtų būti saugomos (apsaugotos šifravimo priemonėmis) ir reguliariai testuojamos pagal sutartą konkretaus dalyko politiką, o atsarginių kopijų atkūrimo procedūros žingsniai dokumentuoti.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS, dokumentais pagrįstos, atsarginių kopijų kūrimo ir atkūrimo politikos, daro išvadą, kad 89 proc. Įstaigų įgyvendino išsamią ir dokumentais pagrįstą atsarginių kopijų (dalinių / pilnų) kūrimo ir atkūrimo politiką.

2. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų duomenys visa apimtimi įtraukiami į atsarginių kopijų kūrimą. Gairių 134 punkte pateiktos nuostatos yra skirtos atsarginių kopijų darymui (apimtis / dažnumas). Gairėse nurodyta, kad atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą. Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų darymo, daro išvadą, kad 100 proc. Įstaigų duomenis visa apimtimi įtraukia į atsarginių kopijų kūrimą.

3. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų kasdien daromos atsarginės kopijos. Gairių 134 punkte pateiktos nuostatos yra skirtos atsarginių kopijų darymui (apimtis / dažnumas). Gairėse nurodyta, kad atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą. Rekomenduojamas atsarginių kopijų darymo dažnumas: kasdien – pridedamoji kopija; kas savaitę – pilna kopija.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų darymo, daro išvadą, kad 100 proc. Įstaigų visa apimtimi duomenis įtraukia į atsarginių kopijų kūrimą: kasdien – pridedamoji kopija; kas savaitę – pilna kopija.

4. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų naudoja automatizuotus sprendimo metodus atsarginėms kopijoms kurti. Aprašo V skirsnyje „Veiklos tęstinumas“ nurodyta, kad atsarginės kopijos turi būti reguliariai testuojamos įgalioto asmens arba turi būti naudojama speciali programinė įranga, kuri automatiškai patikrina, ar iš duomenų kopijos galima atkurti duomenis, kurie būtų visiškai funkcionalūs. Nacionalinio kibernetinio saugumo centro (toliau – NKSC) „Kibernetinio saugumo centro rekomendacijos kibernetinio saugumo subjektams“[6] rekomendacijų 11 papunktyje „Duomenų atkūrimas (angl. *Data Recovery*)“ nurodyta, kad atsarginėms kopijos kurti būtų naudojami automatizuoti sprendimai.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS metodų atsarginėms kopijoms kurti, daro išvadą, kad 100 proc. Įstaigų naudoja automatizuotus sprendimo metodus atsarginėms kopijoms kurti.

5. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų atsargines kopijas saugo vietiniuose serveriuose (kitame korpuse), naudojantis debesijos paslaugomis, išorinėse laikmenose, virtualiose mašinose. Gairių 132, 136, punktuose pateiktos nuostatos yra skirtos atsarginių kopijų saugojimui ir jų laikmenoms. Gairėse nurodyta, kad atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų. Taip pat atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų saugojimo, daro išvadą, kad 100 proc. Įstaigų saugo atsargines kopijas vietiniuose serveriuose (kitame korpuse), naudoja debesijos paslaugas, išorinėse laikmenose, virtualiose mašinose.

6. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų atsarginės kopijos šifruojamos, siekiant apsaugoti jautrius (specialiųjų kategorijų) duomenis. Gairių 137 punkte pateiktos nuostatos yra skirtos atsarginių kopijų šifravimui. Gairėse nurodyta, kad atsarginės kopijos turi būti šifruojamos ir saugiai laikomos visiškai atjungus (angl. *Offline*) nuo kompiuterinių tinklų. Aprašo X skirsnyje „Kriptografijos ir šifravimo naudojimo politika ir procedūros“ nurodyta, kad duomenys atsarginėse kopijose turi būti užšifruoti (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų informacijai neteisėtai atkurti.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų šifravimo, daro išvadą, kad 100 proc. Įstaigų atsarginės kopijos šifruojamos, siekiant apsaugoti jautrius (specialiųjų kategorijų) duomenis.

[6] https://www.nksc.lt/doc/NKSC_rekomendacijos_kibernetinio_saugumo_subjektams.pdf

7. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų naudoja geografiškai atskirtas atsarginių kopijų saugyklas, siekiant išvengti duomenų praradimo incidento atveju. Gairių 136 punkte pateiktos nuostatos yra skirtos atsarginių kopijų saugojimui. Gairėse nurodyta, kad atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos. Aprašo V skirsnyje „Veiklos tęstinumas“ nurodyta, kad kibernetinio saugumo subjekto nustatyta tvarka ir nustatytu reguliarumu turi būti daromos atsarginės duomenų kopijos ir turi būti laikomos geografiškai nutolusioje vietoje. ISO standarto 8.13 papunktyje „Informacijos atsarginės kopijos“ nurodyta, kad atsarginių kopijų saugojimas turi būti saugioje ir patikimoje vietoje, nutolusioje pakankamu atstumu, kad būtų išvengta bet kokios žalos dėl nelaimės pagrindiniame objekte.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų saugojimo, daro išvadą, kad 100 proc. Įstaigų naudoja geografiškai atskirtas atsarginių kopijų saugyklas, siekdamos išvengti duomenų praradimo incidento atveju.

8. Stebėsenų atlikimo metu nustatyta, kad 89 proc. Įstaigų prieigą prie atsarginių kopijų turi tik įgalioti asmenys. Aprašo V skirsnyje „Veiklos tęstinumas“ nurodyta, kad atsarginės kopijos turi būti reguliariai testuojamos įgalioto asmens arba turi būti naudojama speciali programinė įranga, kuri automatiškai patikrina, ar iš duomenų kopijos galima atkurti duomenis, kurie būtų visiškai funkcionalūs.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų prieigos, daro išvadą, kad 89 proc. Įstaigų prieigą prie atsarginių kopijų turi tik įgalioti asmenys.

9. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų periodiškai tikrinamas / testuojamas atsarginių kopijų atkūrimo procesas. Gairių 135 punkte pateiktos nuostatos yra skirtos atsarginių kopijų tikrinimui / testavimui. Gairėse nurodyta, kad atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje. Aprašo V skirsnyje „Veiklos tęstinumas“ nurodyta, kad atsarginės kopijos turi būti reguliariai testuojamos įgalioto asmens arba turi būti naudojama speciali programinė įranga, kuri automatiškai patikrina, ar iš duomenų kopijos galima atkurti duomenis, kurie būtų visiškai funkcionalūs.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų tikrinimo / testavimo, daro išvadą, kad 100 proc. Įstaigų periodiškai tikrinamas / testuojamas atsarginių kopijų atkūrimo procesas.

10. Stebėsenų atlikimo metu nustatyta, kad 100 proc. Įstaigų testavimo metu atkuriami visi svarbiausi duomenys be praradimų. ISO standarto 8.13 papunktyje „Informacijos atsarginės kopijos“ nurodyta, kad turi būti reguliarus atsarginių laikmenų išbandymas, siekiant užtikrinti, kad prireikus jomis būtų galima pasikliauti ir naudoti kritiniu atveju. Testavimu turi būti patvirtinama, kad atsarginės kopijos gali būti atkurtos bandomoje aplinkoje neperrašant originalios laikmenos, taip sumažinant riziką, kad nesėkmingo atsarginių kopijų darymo ar atkūrimo proceso metu duomenys būtų nepataisomai sugadinti ar prarasti.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų atkūrimo testavimo metu, daro išvadą, kad 100 proc. Įstaigų testavimo metu atkuriami visi svarbiausi duomenys be praradimų.

11. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų atsarginių kopijų atkūrimo procedūros žingsniai dokumentuoti. ISO standarto 8.13 papunktyje „Informacijos atsarginės kopijos“ nurodyta, kad turi būti dokumentuoti tikslūs ir išsamūs atsarginių kopijų atkūrimo procedūros žingsniai. Turi būti numatytos tinkamos atsarginių kopijų darymo priemonės, dokumentuoti atkūrimo procedūros žingsniai, užtikrinantys, kad įvykus incidentui, sutrikimui ar praradus laikmenas būtų galima atkurti visą svarbiausią informaciją ir programinę įrangą.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų atkūrimo procedūros, daro išvadą, kad 78 proc. Įstaigų atsarginių kopijų atkūrimo procedūros žingsniai dokumentuoti.

12. Stebėsenų atlikimo metu nustatyta, kad Įstaigose atsarginės kopijos saugomos nuo 14 dienų iki 5 metų. BDAR 32 straipsnio 1 dalies c punkte reglamentuota, kad organizacija turi gebėti laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS atsarginių kopijų saugojimo termino, daro išvadą, kad Įstaigose atsarginių kopijų saugojimo terminas atitinka gerąją tarptautinę praktiką.

Žurnaliniai įrašai

1. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų turi žurnalinių įrašų (angl. *Logs*) valdymo politikas. ISO standarto 5.37 papunktyje „Dokumentuotos veiklos procedūros“ nurodyta, kad informacijos apdorojimo priemonių naudojimo procedūros turėtų būti dokumentuotos ir prieinamos personalui, kuriam jų reikia. Turėtų būti parengtos dokumentuotos procedūros organizacijos operatyviniams veiksmams, susijusiems su informacijos saugumu – audito sekų ir sistemos žurnalinių įrašų informacijos valdymu.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų valdymo politikos, daro išvadą, kad 78 proc. Įstaigų įgyvendino žurnalinių įrašų valdymo politiką.

2. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų žurnalinių įrašų valdymo politika peržiūrima ir atnaujinama reguliariai. ISO standarto 5.37 papunktyje „Dokumentuotos veiklos procedūros“ nurodyta, kad dokumentuotos veiklos procedūros turėtų būti peržiūrimos ir prireikus atnaujinamos. Dokumentuotų veiklos procedūrų pakeitimai turėtų būti patvirtinti. Jei techniškai įmanoma, IS turėtų būti valdomos nuosekliai, naudojant tas pačias procedūras, priemones ir įrankius.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų valdymo politikos peržiūros ir atnaujinimo, daro išvadą, kad 78 proc. Įstaigų reguliariai peržiūri ir atnaujina žurnalinių įrašų valdymo politiką.

3. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų fiksuoja visus vidinius ir išorinius įvykius žurnaliniuose įrašuose. Gairių 117 punkte pateiktos nuostatos yra skirtos žurnaliniuose įrašuose įvykių registravimui. Gairėse nurodyta, kad techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz.: data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad žurnaliniuose įrašuose turi būti fiksuojami bent jau šie žurnaliniai įrašai (jei tinklų ir IS dalys palaiko tokį funkcionalumą):

- tinklų ir IS komponentų (serverių, virtualių serverių, saugiasienių, maršrutizatorių, komutatorių ir kitų subjekto identifikuotų svarbių komponentų) įjungimas, išjungimas ar perkrovimas;
- naudotojų ir administratorių autentifikavimo įvykiai;
- naudotojų, administratorių paskyrų sukūrimas, prieigų prie tinklų ir IS pakeitimai;
- administratorių atliekami veiksmai;
- operacinėse sistemose sukurti ir atlikti sisteminiai uždavinių įvykiai (angl. *Scheduled task*);
- grupinių politikų pakeitimai;
- saugiasienių taisyklių pakeitimai;
- žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas;
- operacinių sistemų laiko ir datos pakeitimai;
- saugumo sistemų (antivirusinių, įsibrovimo aptikimo sistemų) įjungimas ir išjungimas;
- operacinėse sistemose vykstančių procesų ar servisų įvykiai;
- tinklų ir IS galinių įrenginių autentifikavimo įvykiai;
- žurnalinių įrašų peržiūrėjimas, trynimas, kūrimas ar keitimas.

Tinklai ir IS turi turėti ne mažiau kaip 2 laiko šaltinius. Žurnaliniuose įrašuose turi būti fiksuojami bent jau šie duomenys (jei tinklų ir IS dalys palaiko tokį funkcionalumą)*:*

- įvykio data ir tikslus laikas;
- įvykio rūšis (informacija, klaida, saugumo pranešimas, sisteminis pranešimas, perspėjimas (angl. *Warning*);
- naudotojo / administratoriaus ir (arba) tinklų ir IS įrenginio, susijusio su įvykiu, identifikavimo duomenys;
- įvykio aprašymas.

Priemonės, naudojamos vidinės tinklų ir IS sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad žurnaliniuose įrašuose fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais. Tinklų ir IS fiksuojami žurnaliniai įrašai turi būti saugomi specializuotoje tam pritaikytoje techninėje ar programinėje įrangoje. Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant (automatiniu pranešimu (angl. *Alert*), bet ne vėliau kaip per vieną darbo dieną, turi būti informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS fiksuojamų įvykių žurnaliniuose įrašuose, daro išvadą, kad 78 proc. Įstaigų žurnaliniuose įrašuose fiksuoja visus vidinius ir išorinius įvykius.

4. Stebėsenų atlikimo metu nustatyta, kad 67 proc. Įstaigų žurnalinius įrašus saugo ne trumpiau kaip 90 kalendorinių dienų. Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 90 kalendorinių dienų.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų saugojimo termino, daro išvadą, kad 67 proc. Įstaigų žurnalinius įrašus saugo ne trumpiau kaip 90 kalendorinių dienų.

5. Stebėsenų atlikimo metu nustatyta, kad 56 proc. Įstaigų žurnalinius įrašus saugo centralizuotai. Aprašo VII skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad kibernetinio saugumo subjekto serveriuose ir kompiuterinėse darbo vietose turi būti naudojamos (jei įmanoma, centralizuotai), valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, stebėjimo realiu laiku priemonės.

Centralizuotas žurnalinių įrašų saugojimas reiškia, kad visi sistemos, tinklo įrenginių, programų ar serverių žurnaliniai įrašai kaupiami vienoje centralizuotoje vietoje – žurnalinių įrašų valdymo sistemoje.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų saugojimo budo, daro išvadą, kad 56 proc. Įstaigų žurnalinius įrašus saugo centralizuotai.

6. Stebėsenų atlikimo metu nustatyta, kad 89 proc. Įstaigų žurnaliniams įrašams taiko prieigos valdymo kontrolę (nuo neautorizuotos prieigos ar žurnalinių įrašų pakeitimo). Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad naudojimasis žurnaliniais įrašais turi būti kontroliuojamas ir fiksuojamas, žurnaliniai įrašai turi būti pasiekiami tik kibernetinio saugumo subjekto įgaliotiems asmenims ir kibernetinio saugumo vadovui (peržiūros teisėmis). Žurnalinių įrašų duomenys turi būti analizuojami įgalioto asmens ne rečiau kaip kartą per mėnesį ir apie analizės rezultatų nuokrypius informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų prieigos valdymo kontrolės, daro išvadą, kad 89 proc. Įstaigų žurnaliniams įrašams taiko prieigos valdymo kontrolę (nuo neautorizuotos prieigos ar žurnalinių įrašų pakeitimo).

7. Stebėsenų atlikimo metu nustatyta, kad 56 proc. Įstaigų žurnalinius įrašus šifruoja. Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad žurnalinių įrašų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo. ISO standarto 8.15 papunktyje „Registravimas įvykių žurnale“ nurodyta, kad kontrolės priemonėmis turi būti siekiama apsisaugoti nuo neleistinų žurnalinių įrašų informacijos pakeitimų ir siekiant apsaugoti įvykių žurnalus, reikėtų apsvarstyti

galimybę naudoti šifravimo metodus. ISO standarto 8.24 papunktyje „Kriptografijos[7] naudojimas“ nurodyta, kad užtikrinti tinkamą ir veiksmingą kriptografijos naudojimą siekiant apsaugoti informacijos konfidencialumą, autentiškumą ar vientisumą pagal veiklos ir informacijos saugumo reikalavimus bei atsižvelgiant į teisinius, įstatyminius, reguliavimo ir sutartinius reikalavimus, susijusius su kriptografija. Informacijos šifravimas naudojamas siekiant apsaugoti saugomą arba perduodamą neskelbtiną arba svarbią informaciją.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų apsaugos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo, daro išvadą, kad 56 proc. Įstaigų žurnaliniams įrašams apsaugoti taiko šifravimo metodus.

8. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų žurnalinių įrašų pakeitimus stebi ir registruoja. ISO 8.9 papunktyje „Konfigūracijų valdymas“ papunktyje nurodyta, kad turi būti nustatytos, dokumentuotos, įgyvendintos, stebimos ir peržiūrimos techninės įrangos, programinės įrangos, paslaugų ir tinklų konfigūracijos, įskaitant saugumo konfigūracijas. Organizacijoje turi būti registruojamos nustatytos techninės ir programinės įrangos, paslaugų ir tinklų konfigūracijos, o visi konfigūracijos pakeitimai turėtų būti registruojami įvykių žurnale. Šie įrašai turėtų būti saugiai saugomi.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų pakeitimo, daro išvadą, kad 78 proc. Įstaigų žurnalinių įrašų pakeitimus stebi ir registruoja.

9. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų žurnalinių įrašų peržiūrą atlieka ne rečiau kaip kartą per mėnesį. Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad žurnalinių įrašų duomenys turi būti analizuojami įgalioto asmens ne rečiau kaip kartą per mėnesį ir apie analizės rezultatų nuokrypius informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų peržiūros, daro išvadą, kad 78 proc. Įstaigų žurnalinių įrašų peržiūrą atlieka ne rečiau kaip kartą per mėnesį.

10. Stebėsenų atlikimo metu nustatyta, kad 67 proc. Įstaigų įdiegusios automatinius įspėjimus (angl. *Alerts*) apie įtartinus ar neįprastus įvykius (pvz., neįprasti prisijungimai ar duomenų peržiūra). Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad neįprasta veikla turi būti užfiksuojama žurnaliniuose įrašuose ir, jei įmanoma, automatizuotomis priemonėmis sukuriamas automatinis pranešimas, kurį matytų kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS automatinių įspėjimų, daro išvadą, kad 67 proc. Įstaigų įdiegusios automatinius įspėjimus (angl. *Alerts*) apie įtartinus ar neįprastus įvykius (pvz., neįprasti prisijungimai ar duomenų peržiūra).

[7] https://www.vle.lt/straipsnis/kriptografija/

11. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų atlieka reguliarius žurnalinių įrašų auditus, siekdamos patikrinti, ar juose nėra įtartinos veiklos. Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad žurnalinių įrašų duomenys turi būti analizuojami įgalioto asmens ne rečiau kaip kartą per mėnesį ir apie analizės rezultatų nuokrypius informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis. ISO 8.16 papunktyje „Stebėsenos veikla“ papunktyje nurodyta, kad stebėsena turi apimti įvykių žurnalus, susijusius su sistemos ir tinklo veikla, o automatizuota stebėsenos programinė įranga turėtų būti sukonfigūruota taip, kad pagal iš anksto nustatytus kriterijus būtų generuojami įspėjimai (pvz., per valdymo pultus, el. pašto pranešimus ar per žinučių sistemas).

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS reguliarų žurnalinių įrašų auditų, daro išvadą, kad 78 proc. Įstaigų atlieka reguliarius žurnalinių įrašų auditus, siekdamos patikrinti, ar juose nėra įtartinos veiklos.

12. Stebėsenų atlikimo metu nustatyta, kad 78 proc. Įstaigų žurnalinių įrašų valdymo procesas yra dokumentuotas. Aprašo IV skirsnyje „Kibernetinių incidentų valdymas“ nurodyta, kad naudojimasis žurnaliniais įrašais turi būti kontroliuojamas ir fiksuojamas. Žurnaliniai įrašai turi būti pasiekiami tik kibernetinio saugumo subjekto įgaliotiems asmenims ir kibernetinio saugumo vadovui (peržiūros teisėmis).

Inspekcija, įvertinusi Įstaigų pateiktą informaciją ir įrodymus dėl IS žurnalinių įrašų valdymo proceso, daro išvadą, kad 78 proc. Įstaigų žurnalinių įrašų valdymo procesas yra dokumentuotas.

Saugumo priemonių įgyvendinimo lygio įvertinimas pagal rizikos zonas

Rizikos lygis	Sritis / priemonė	Įstaigų stebėsenų rezultatas
[8]	Kelių veiksnių autentifikacija (angl. MFA)	**89 proc.**
	Centralizuotas žurnalinių įrašų saugojimas	**56 proc.**
	Žurnalinių įrašų šifravimas	**56 proc.**
	Automatiniai įspėjimai (angl. *Alerts*) apie įtartinus įvykius	**67 proc.**
	Žurnalinių įrašų saugojimas ≥ 90 dienų	**67 proc.**
[9]	Žurnalinių įrašų valdymo politika	**78 proc.**
	Žurnalinių įrašų valdymo politikos peržiūra ir atnaujinimas	**78 proc.**
	Vidinių ir išorinių įvykių fiksavimas žurnaliniuose įrašuose	**78 proc.**
	Žurnalinių įrašų pakeitimų stebėsena ir registravimas	**78 proc.**

[8] **Kritinės spragos**, kurios kelia didelę riziką asmens duomenų saugumui ir reikalauja neatidėliotinų valdymo bei techninių sprendimų.

[9] **Reikšmingos spragos**, kurios neturi tiesioginio kritinio poveikio, tačiau turėtų būti pašalintos artimiausiu laikotarpiu, siekiant sumažinti riziką ir užtikrinti atitiktį teisės aktams.

	Reguliarūs žurnalinių įrašų auditai	**78 proc.**
	Žurnalinių įrašų valdymo proceso dokumentavimas	**78 proc.**
[10]	IS naudotojų prieigos teisių dokumentavimas	**11 proc.**
	Individualių naudotojų paskyrų taikymas (nebendrinamos prieigos)	**11 proc.**
	Prieigos prie atsarginių kopijų ribojimas tik įgaliotiems asmenims	**11 proc.**
	Atsarginių kopijų atkūrimo procedūrų žingsnių dokumentavimas	**22 proc.**
[11]	Privilegijuotųjų prieigos teisių kontrolė	**100 proc.**
	Naudotojų veiksmų registravimas įvykių žurnaluose	**100 proc.**
	Duomenų įtraukimas į atsarginių kopijų kūrimą	**100 proc.**
	Atsarginių kopijų kūrimo reguliarumas (kasdien / kas savaitę)	**100 proc.**
	Automatizuotas atsarginių kopijų kūrimas	**100 proc.**
	Atsarginių kopijų šifravimas	**100 proc.**
	Geografiškai atskirtos atsarginių kopijų saugyklos	**100 proc.**
	Atsarginių kopijų atkūrimo testavimas	**100 proc.**
	Sėkmingas duomenų atkūrimas testavimo metu	**100 proc.**

Apibendrinant lentelėje pateiktus stebėsenos rezultatus, nustatyta, kad Įstaigose didžioji dalis bazinių techninių ir organizacinių saugumo priemonių yra įgyvendintos, ypač atsarginių kopijų kūrimo, duomenų šifravimo ir veiklos tęstinumo užtikrinimo srityse. Tačiau stebėsena atskleidė reikšmingas spragas prieigos valdymo ir žurnalinių įrašų srityse, visų pirma susijusias su kelių veiksnių autentifikacijos taikymu, žurnalinių įrašų centralizavimu, šifravimu ir automatizuotu įspėjimų naudojimu. Atsižvelgiant į tai, kad Įstaigos tvarko specialiųjų kategorijų asmens (sveikatos) duomenis, rekomenduojama prioritetą teikti raudonos ir oranžinės zonų priemonių įgyvendinimui, nuosekliai stiprinant saugumo kontrolę, dokumentavimo procesus ir nuolatinę stebėseną, siekiant užtikrinti atitiktį BDAR ir kibernetinio saugumo reikalavimams.

[10] **Vidutinės rizikos sritys**, kuriose taikomos saugumo priemonės, tačiau būtinas jų tobulinimas, dokumentavimas ar nuoseklesnis taikymas.

[11] **Įgyvendintos saugumo priemonės ir gera praktika**, atitinkanti teisės aktų bei rekomendacijų reikalavimus; rekomenduojama palaikyti ir periodiškai peržiūrėti.