

2026

Planinės stebėsenos
rezultatatai

Planinės stebėsenos rezultatai

Kontrolinio klausimyno apibendrinimas: prieigos teisės,
atsarginės kopijos ir žurnaliniai įrašai 10 įstaigų

10 įstaigų

3 saugumo sritys

28 kontroliniai klausimai

Apimtis ir metodika

Vertinimo objektas

Kontrolinis saugumo priemonių klausimynas, užpildytas kiekvienos įstaigos IT atsakingų darbuotojų.

Trys sritys

Prieigos teisės, atsarginių kopijų valdymas ir žurnalinių įrašų (angl. *Log*) tvarkymas.

Įrodymai

Prie atsakymų prašyta pateikti juos pagrindžiančius įrodymus (pvz., dokumentus / technines konfigūracijas).

Vertinimo principas

Atsakymai „Taip“ laikyti įgyvendinta priemone; „Ne“ su paaiškinimu – daline arba kompensuojama priemone. Rezultatai pateikiami apibendrintai, nenurodant įstaigų pavadinimų.

Bendras rezultatas

Prieigos teisės

Stipriausia sritis

Atsarginės kopijos

Gera branda

Žurnaliniai įrašai

Tobulintina sritis

Visiškai įgyvendintos priemonės (įstaigų skaičius iš 10)

Individualios naudotojų ir administratorių paskyros

10/10

Automatizuotas atsarginių kopijų kūrimas

10/10

Dokumentuota žurnalinių įrašų valdymo politika

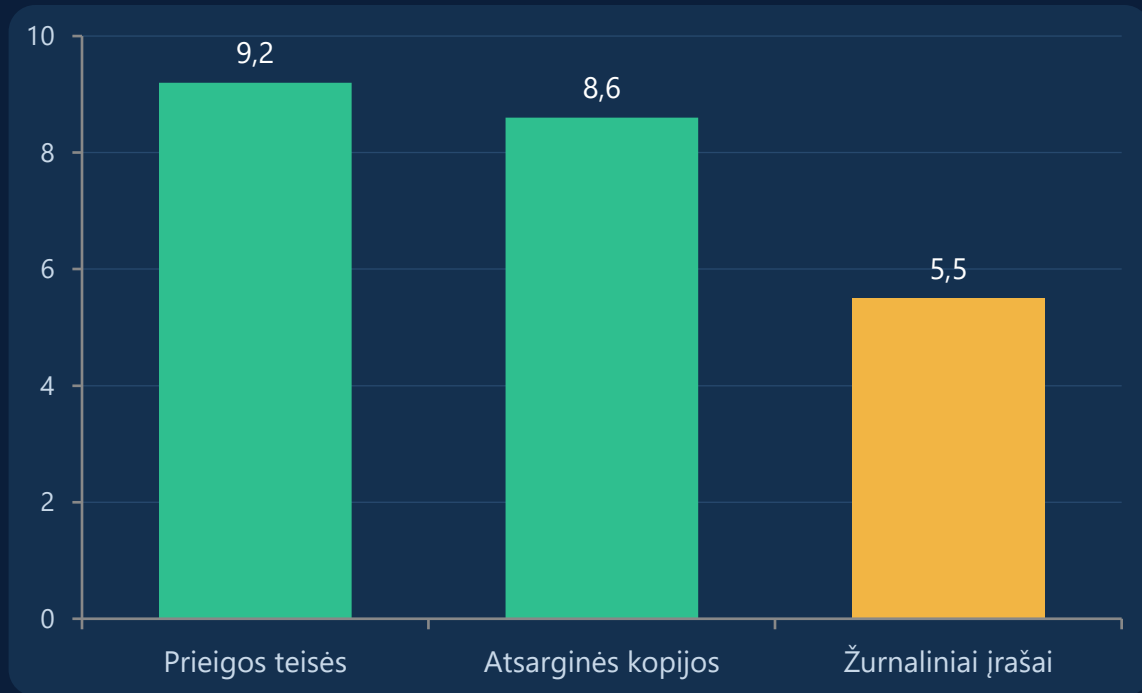
7/10

Centralizuotas žurnalinių įrašų kaupimas

5/10

DIAGRAMA

Igyvendinimo lygis pagal sritis



Kaip apskaičiuota

Kiekvienos srities rodiklis yra vidutinis įstaigų, visiškai įgyvendinusių tos srities priemones, skaičius iš 10.

Žurnalinių įrašų sritis atsilieka nuo kitų dviejų maždaug trečdaliu.

Prieigos teisės

Bendrinės naudotojų paskyros nenaudojamos 10/10



Individualios administratorių paskyros 10/10



Kelių faktorių autentifikacija (MFA) 9/10



Dokumentuotas prieigos teisių suteikimas 8/10



Naudotojų veiksmai registruojami įvykių žurnaluose 9/10

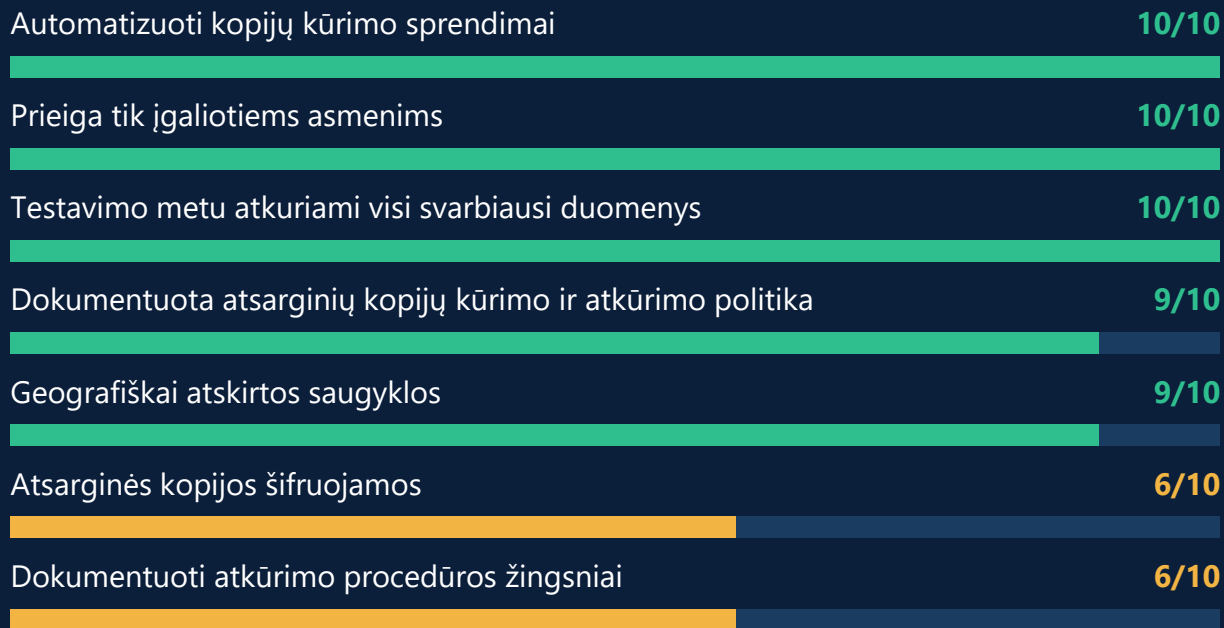


Ką rodo atsakymai

- IS naudotojų prieigos teisės nėra bendrinamos ar susiejamos su keliais asmenimis
- Dvi įstaigos dokumentuoja prieigų suteikimą tik per grupes ar vadovo prašymu
- MFA vienoje įstaigoje veikia tik daliai sistemų dėl techninių apribojimų

Branda: aukšta. **Pagrindinis trūkumas** – formalus dokumentavimas, o ne techninė kontrolė.

Atsarginės kopijos: pagrindiniai rodikliai



4 įstaigos kopijų nešifruoja, nurodydamos, kad specialiųjų kategorijų duomenų netvarko ir taiko fizines bei technines apsaugos priemones.

4

įstaigos neturi
dokumentuotų atkūrimo
žingsnių

2

atkūrimą testuoja tik „pagal
poreikį“, be periodiškumo

Atsarginių kopijų praktika

Apimtis

Dažniausiai kopijuojamos visos virtualios mašinos su operacinėmis sistemomis, duomenų bazėmis ir konfigūracijomis t. y. pilna apimtis.

Dažnis

Nuo kasdienių inkrementinių kopijų iki 6 kartų per parą kritinėms sistemoms, o pilnos kopijos kartą per savaitę.

Saugojimo vieta

Vyrauja vietiniai serveriai nutolusiuose duomenų centruose, papildomai – debesijos paslaugos ir offline laikmenos.

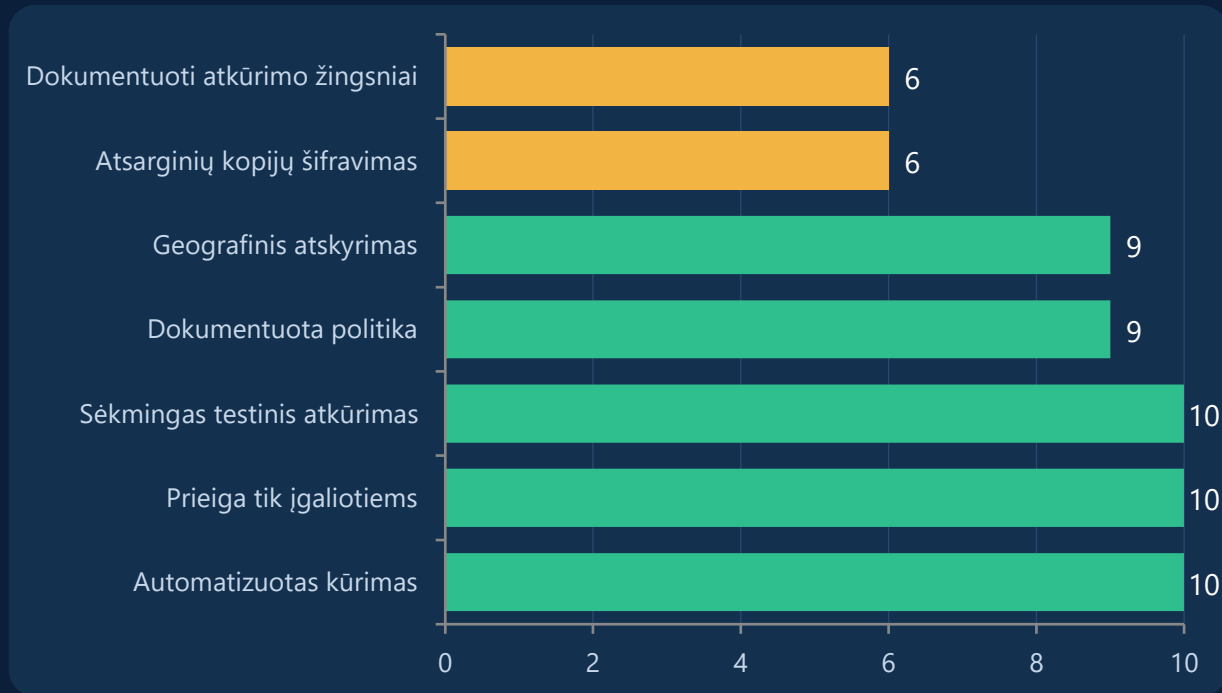
Saugojimo trukmė

Labai skirtinga: nuo 3 parų iki 5 metų. Dalis įstaigų taiko diferencijavimą pagal sistemų kritiškumą.

Nė viena įstaiga nenurodė rankinio kopijų kūrimo – **visos naudoja automatizuotus sprendimus.**

DIAGRAMA

Atsarginių kopijų priemonės diagramoje



Išvalga

Techninės priemonės įdiegtos beveik visur, tačiau dokumentavimas ir šifravimas atsilieka – būtent ten susidaro atotrūkis.

Žurnaliniai įrašai: atitiktis reikalavimams

Saugojimo trukmė – ne trumpiau kaip 90 kalendorinių dienų

7 iš 10 įstaigų atitinka. Viena saugo 60 d., viena neturi formaliai nustatyto termino, dar vienos dalis debesijos žurnalų saugoma tik mėnesį.

Peržiūra – ne rečiau kaip kartą per mėnesį

Tik 5 įstaigos peržiūri reguliariai (realiu laiku, kasdien ar savaitiskai). Kitos tik „pagal poreikį“, sprendžiant incidentus.

Įgyvendintos žurnalinių įrašų priemonės (iš 10)

Prieiga prie žurnalinių įrašų kontrolė

10/10

Žurnalinių įrašų valdymo politika

7/10

Automatiniai įspėjimai apie įtartinus įvykius

6/10

Centralizuotas arba hibridinis kaupimas

5/10

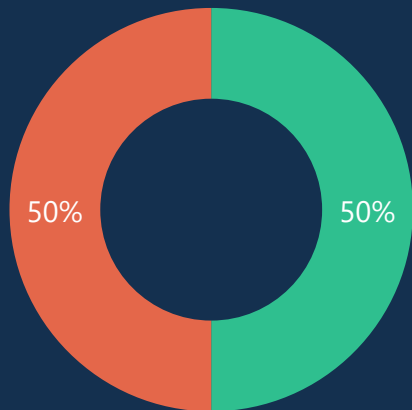
Žurnalinių įrašų pakeitimų stebėsena ir registravimas

3/10

DIAGRAMA

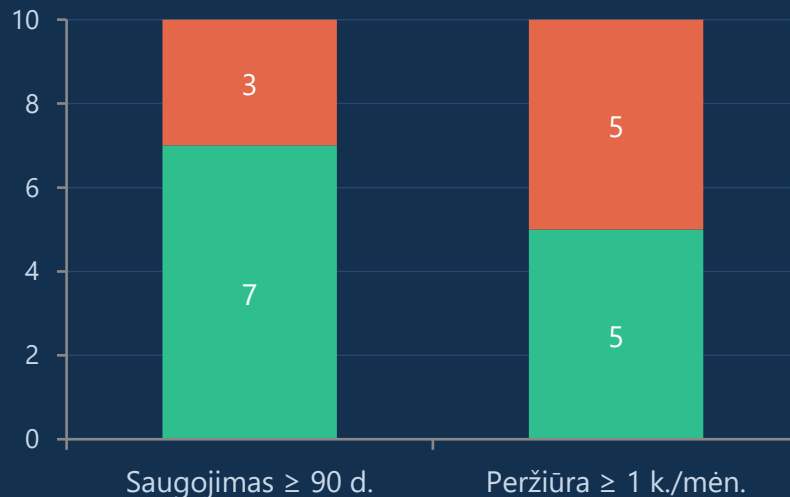
Žurnalinių įrašų pjūvis diagramose

Žurnalinių įrašų saugojimo modelis



■ Centralizuotai arba hibridiškai ■ Išskaidyta tarp sistemų

Žurnalinių įrašų saugojimo ir peržiūros atitiktis



■ Atitinka ■ Neatitinka

Žurnalinių įrašų spragos

6/10

automatiniai įspėjimai apie įtartinus įvykius

3/10

stebi ir registruoja žurnalinių įrašų pakeitimus

4/10

atlieka reguliarius žurnalinių įrašų auditus

6/10

turi dokumentuotą žurnalinių įrašų valdymo procesą

Kontekstas

Dalis įstaigų nurodo kompensuojamąsias priemones: įrašų keitimas techniškai neįmanomas, prieiga ribojama teisėmis, o analizė atliekama incidentų metu. Tačiau be centralizuoto kaupimo ir vientisumo kontrolės šios priemonės nėra patikrinamos.

Pagrindinės rizikos

Aukšta**Decentralizuoti žurnaliniai įrašai**

Pusė įstaigų kaupia žurnalinius įrašus atskirose sistemose – incidento tyrimas lėtas, o piktavališkas gali ištrinti vietinius žurnalinius įrašus.

Aukšta**Neužtikrintas žurnalinių įrašų vientisumas**

Septynios įstaigos nestebi žurnalinių įrašų pakeitimų, todėl įrodomoji vertė audito / incidento metu ribota.

Vidutinė**Nedokumentuotas duomenų atkūrimas**

Keturios įstaigos neturi aprašytos duomenų atkūrimo tvarkos, todėl atkūrimas priklauso nuo pavienių darbuotojų patirties.

Vidutinė**Nereguliari stebėseną**

Peržiūra ir auditai atliekami „pagal poreikį“, todėl lėti, ilgai besitęsiantys incidentai gali likti nepastebėti.

Rekomendacijos ir kiti žingsniai

01 Centralizuoti žurnalinius įrašus

Įdiegti bendrą žurnalinių įrašų kaupimo serverį ar SIEM sprendimą, užtikrinant įrašų vientisumą ir automatinius perspėjimus.

02 Formalizuoti trūkstamas politikas

Patvirtinti žurnalinių įrašų valdymo politiką ir dokumentuoti atsarginių kopijų atkūrimo žingsnius ten, kur jų nėra.

03 Nustatyti periodiškumą

Įtvirtinti ne rečiau kaip mėnesinę žurnalinių įrašų peržiūrą, reguliarių atkūrimo testavimą ir 90 dienų saugojimo minimalu terminą.

04 Sustiprinti vientisumo kontrolę

Šifruoti atsargines kopijas, stebėti žurnalinių įrašų pakeitimus, užbaigti geografinį atskyrimą.