„KIBERNETINIO SAUGUMO UŽTIKRINIMAS"

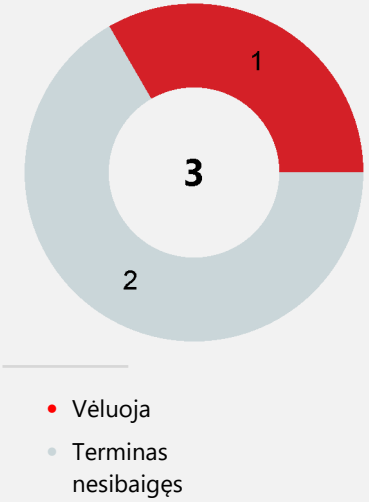
Valstybinio audito ataskaita: 2022-10-27 Nr. VAE-10

Rekomendacijų stebėsenos ataskaita

2026-09-09 13:24

Teikta

Laukia įgyvendinimo



„KIBERNETINIO SAUGUMO UŽTIKRINIMAS"

Valstybinio audito ataskaita: 2022-10-27 Nr. VAE-10

Rekomendacijų stebėsenos ataskaita

2026-09-09 13:24

Rekomendacija / priemonė	Iki kada turi būti įgyvendinta	Būklė	Laiko būklė
1 rekomendacija: Siekiant užtikrinti kibernetinės apsaugos, prevencijos ir atsako priemonių panaudojimą, turi būti diegiamas ir nacionaliniu mastu koordinuojamas informacinių technologijų saugumo rizikų (įskaitant kibernetines) valdymo procesas, kuris leistų gautą informaciją apie kibernetinio saugumo rizikingumo būklę naudoti priimant strateginius sprendimus dėl kibernetinio saugumo stiprinimo.	2028-12-31	Laukiama įgyvendinimo	Terminas nesibaigęs

Atsakingas subjektas:
Lietuvos Respublikos krašto apsaugos ministerija

Rodiklis

Nacionalinei stebėsenos sistemai IT saugumo rizikos vertinimus pateikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis

Pradinė reikšmė: proc. (2021 m.)

Siektina reikšmė: 100 proc. (2028 m.)

Rodiklis

Nacionalinio kibernetinio saugumo centro atliktų atitikties saugumo reikalavimams, taikomiems valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams ir ypatingos svarbos informacinės infrastruktūros valdytojams, vertinimų dalis

Pradinė reikšmė: proc. (2021 m.)

Siektina reikšmė: 70 proc. (2028 m.)

Rodiklis

Sudarytas ir kasmet atnaujinamas nacionalinis kibernetinio saugumo rizikos profilis

Pradinė reikšmė: Nesudarytas (2022 m.)

Siektina reikšmė: Sudarytas ir kasmet atnaujinamas (2028 m.)

1 priemonė: Nustatyti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše reikalavimą valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams, ypatingos svarbos informacinės infrastruktūros valdytojams teikti atliktų ryšių ir informacinių sistemų rizikos vertinimų ataskaitas nacionalinei stebėsenos sistemai.	2024-12-31	Įgyvendinta	Laiku

Atsakingas subjektas:
Lietuvos Respublikos krašto apsaugos ministerija

Rekomendacijų stebėsenos ataskaita

2026-09-09 13:24

Rekomendacija / priemonė	Iki kada turi būti įgyvendinta	Būklė	Laiko būklė
Rezultatas: 2023-07-19 priimti teisės aktų pakeitimai (LRV nutarimas Nr. 573 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ pakeitimo“, LRV nutarimas Nr. 574 „Dėl Lietuvos Respublikos Vyriausybės 2018-08-13 nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“, LRB nutarimas Nr. Nr. 575 „„Dėl Lietuvos Respublikos Vyriausybės 1998-07-23 nutarimo Nr. 924 „Dėl Lietuvos Respublikos krašto apsaugos ministerijos nuostatų patvirtinimo“ pakeitimo“), kuriais nustatyta, kad kibernetinio saugumo subjektai ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių turi atlikti rizikos vertinimą ir jį paskelbti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemoje.			
2 priemonė: Remiantis nacionalinei stebėsenos sistemai pateiktais ryšių ir informacinių sistemų rizikos vertinimų duomenimis, atlikti nacionalinio lygio kibernetinio saugumo rizikų vertinimą ir analizę, sudaryti sektorių rizikos profilius. **Atsakingas subjektas:** Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos **Rezultatas:** Parengta atnaujinta kibernetinio saugumo rizikos vertinimo metodika, kuri yra įkelta į KSIS GRC modulį ir yra pasiekiama atsisiuntimui KSS (KSS gali atsisiųsti rizikos vertinimo metodikos aprašymą, rizikos vertinimo lenteles reikalingas atlikti rizikos vertinimą, bei mokymų medžiagą). Iki 2026 balandžio mėn. planuojamas GRC modulyje įdiegti funkcionalumą, kad rizikos vertinimą būtų galima atlikti tiesiogiai GRC sistemoje, vykdomi programavimo, diegimo ir testavimo darbai.	2027-12-31	Laukiama įgyvendinimo	Terminas nesibaigęs

„KIBERNETINIO SAUGUMO UŽTIKRINIMAS"

Valstybinio audito ataskaita: 2022-10-27 Nr. VAE-10

Rekomendacijų stebėsenos ataskaita

2026-09-09 13:24

Rekomendacija / priemonė	Iki kada turi būti įgyvendinta	Būklė	Laiko būklė
2 rekomendacija: Siekiant kibernetinio saugumo subjektams efektyviau įgyvendinti teisės aktuose nustatytus saugumo reikalavimus, sukurti bendrą kibernetinio saugumo ir informacinių išteklių IT saugos atitikties vertinimo metodiką, sudarančią galimybes atlikti išsamų atitikties teisės aktuose nustatytiems reikalavimams vertinimą ir leisiančią priežiūrą bei stebėseną atliekančiai institucijai rezultatyviau pateikti duomenimis grįstą faktinės būklės nacionalinio lygiu analizę, įžvalgas, apibendrinimą.	2028-12-31	Laukiama įgyvendinimo	Terminas nesibaigęs

Atsakingas subjektas:
Lietuvos Respublikos krašto apsaugos ministerija

Rodiklis

Nacionalinei stebėsenos sistemai IT saugumo rizikos vertinimus pateikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis

Pradinė reikšmė: proc. (2021 m.)

Siektina reikšmė: 100 proc. (2028 m.)

Rodiklis

Nacionalinės stebėsenos sistemos priemonėmis atliktų valstybės informacinių išteklių IT saugumo atitikties vertinimų dalis

Pradinė reikšmė: proc. (2021 m.)

Siektina reikšmė: 100 proc. (2028 m.)

Rodiklis

Nacionalinio kibernetinio saugumo centro atliktų atitikties saugumo reikalavimams, taikomiems valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams ir ypatingos svarbos informacinės infrastruktūros valdytojams, įvertinimų dalis

Pradinė reikšmė: proc. (2021 m.)

Siektina reikšmė: 70 proc. (2028 m.)

1 priemonė: Sukurti bendrą kibernetinio saugumo ir informacinių išteklių IT saugos atitikties vertinimo metodiką.	2026-12-31	Įgyvendinta	Laiku

Atsakingas subjektas:
Lietuvos Respublikos krašto apsaugos ministerija

Rezultatas:
2026 m. vasario 25 d. įsigaliojo įsakymas „Dėl Kibernetinio saugumo auditų atlikimo metodikos patvirtinimo“, kuriuo patvirtinta Kibernetinio saugumo auditų atlikimo metodika ir įtvirtintas vieningas kibernetinio saugumo atitikties vertinimo metodinis pagrindas.

Rekomendacijų stebėsenos ataskaita

2026-09-09 13:24

Rekomendacija / priemonė	Iki kada turi būti įgyvendinta	Būklė	Laiko būklė
2 priemonė: Sukurti bendrą elektroninės informacijos saugos ir kibernetinio saugumo stebėsenos sistemą: 1. Parengti organizacinių ir techninių saugumo reikalavimų nacionalinės stebėsenos sistemos skaitmenino sprendimo įgyvendinimo modelio sukūrimo ir įdiegimo galimybių studiją. 2. Įsigyti, išvystyti ir įdiegti aparatinę ir (arba) programinę įrangą, skirtą skaitmeniniam organizacinių ir techninių saugumo reikalavimų stebėsenos sprendimui įgyvendinti. 3. Sukurti ir įdiegti organizacinių ir techninių saugumo reikalavimų nacionalinės stebėsenos sistemos skaitmeninį sprendimą. **Atsakingas subjektas:** Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos **Rezultatas:** Krašto apsaugos kibernetinio saugumo informacinė sistema sukurta. Sistemos priėmimo ir tinkamumo eksploatuoti aktas 2026 m. birželio 8 d. užregistruotas dokumentų valdymo sistemoje. Veikla (priemonė) įgyvendinta įgyvendinus Ekonomikos gaivinimo ir atsparumo didinimo plano „Naujos kartos Lietuva" (RRF) projektą „Nacionalinės kibernetinio saugumo stebėsenos sistemos sukūrimas".	2027-12-31	Įgyvendinta	Laiku

Rekomendacijų stebėsenos ataskaita

2026-09-09 13:24

Rekomendacija / priemonė	Iki kada turi būti įgyvendinta	Būklė	Laiko būklė
3 rekomendacija: Siekiant sudaryti sąlygas, kad visi kibernetinio saugumo subjektai žinotų veiksmus, kurių reikia imtis įvykus kibernetiniam incidentui ar siekiant užkirsti kelią galimoms grėsmėms: -patvirtinti priemones, kurios užtikrintų sklandesnį komunikavimą apie kibernetinius incidentus naudojantis kibernetinio saugumo informaciniu tinklu; -įpareigoti kibernetinio saugumo subjektus (valstybės informacinių išteklių valdytojus ir tvarkytojus) dalyvauti nacionalinėse kibernetinio saugumo pratybose ir numatyti Nacionalinio kibernetinio saugumo centro vykdomos švietimo veiklos vertinimo rodiklius ir juos periodiškai stebėti; -parengti ir patvirtinti detalų tipinį kibernetinių incidentų valdymo planą ir įpareigoti kibernetinio saugumo subjektus pagal šio standartinio plano pavyzdį parengti ar atnaujinti savo vidinius kibernetinių incidentų valdymo planus / tvarkas.	2025-12-31	Laukiama įgyvendinimo	Vėluoja

Atsakingas subjektas:
Lietuvos Respublikos krašto apsaugos ministerija

Rodiklis

Kibernetinio saugumo subjektų, besinaudojančių kibernetiniu saugumo informaciniu tinklu, dalis

Pradinė reikšmė: 41 proc. (2021 m.)

Siektina reikšmė: 100 proc. (2025 m.)

Rodiklis

Nacionalinėse kibernetinio saugumo pratybose dalyvavusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis

Pradinė reikšmė: proc. (2021 m.)

Siektina reikšmė: 100 proc. (2025 m.)

Rodiklis

Kibernetinių incidentų valdymo planus parengusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis

Pradinė reikšmė: 26 proc. (2022 m.)

Siektina reikšmė: 100 proc. (2025 m.)

1 priemonė: Išvystyti Kibernetinio saugumo informacinio tinklą į naujos kartos tinklą: 1. Atlikti analizę ir nustatyti papildomų paslaugų poreikį kibernetinio saugumo subjektams, siekiant išplėsti Kibernetinio saugumo informacinio tinklo paslaugas ir padidinti jo prieinamumą; 2. Kibernetinio saugumo subjektams suteikti prieigą prie jų infrastruktūroje įdiegtų kibernetinio saugumo priemonių generuojamų duomenų, taip subjektams suteikiant naudą ir sukuriant paskatas naudotis Kibernetinio saugumo informaciniu tinklu.	2023-12-01	Įgyvendinta	Vėlavo

Atsakingas subjektas:
Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos

Rekomendacija / priemonė	Iki kada turi būti įgyvendinta	Būklė	Laiko būklė
Rezultatas: Kibernetinio saugumo informacinio tinklo modernizacija atlikta pasinaudojant RRF projektu. Tinklas pervadintas į Kibernetinio saugumo informacinę sistemą (KSIS). Atnaujinta dalis techninės įrangos, įdiegtas atsarginių kopijų sprendimas ir kt. įranga. Atnaujintas organizacijų portalas, sukurti atitikties, rizikų ir valdysenos (GRC) posistemiai. Kibernetinio saugumo subjektai, prisijungę prie KSIS, be kitų paslaugų gali nemokamai naudotis pratybų įrankiais ir scenarijais, skirtais testuoti darbuotojų atsparumą socialinės inžinerijos principais sukurtoms žinutėms ir tikrinti reagavimo į kibernetinius incidentus valdymo planus. Nemokami kibernetinio saugumo mokymai yra pasiekiami NKSC interneto svetainėje. 2026 m. I pusmetį bent vieną ten esatį kursą jau baigė 33.728 asmenys. Detalus tipinis kibernetinių incidentų valdymo planas yra patvirtintas LRV nutarimu Nr. 818 "Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo". Kibernetinio saugumo subjektai, įgyvendindami organizacinius reikalavimus iki 2026 m. balandžio 17 d. privalėjo pasitvirtinti savo kibernetinių incidentų valdymo planą. Šiuo metu NKSC vykdo patikrinimus, ar šie ir kiti organizaciniai kibernetinio saugumo reikalavimai yra įgyvendinti. Siekiant išplėsti Kibernetinio saugumo informacinio tinklo paslaugas ir padidinti jo prieinamumą buvo atlikti tokie veiksmai: • 2023 m. lapkričio mėn. buvo atliekama Kibernetinio saugumo informacinio tinklo (KSIT) klientų apklausa dėl NKSC teikiamų paslaugų (pridedama); • Parengtas investicijų projektas „Kibernetinio saugumo stebėsenos ir kontrolės sistemos sukūrimas“ (pridedama), kurio tikslas buvo vystyti nacionalinio kibernetinio saugumo priemones, atsižvelgiant į kibernetinėje erdvėje atsirandančias grėsmes ir besikeičiančius valstybės bei visuomenės poreikius, teisės aktus.			
2 priemonė: Nacionalinio kibernetinio saugumo centro strateginiame veiklos plane įvardinti vykdomą švietimo veiklą; šios veiklos vertinimo rodiklius nustatyti centro veiklos plane.	2023-03-01	Įgyvendinta	Vėlavo
Atsakingas subjektas: Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos			
Rezultatas: Patvirtintas 2023 m. Nacionalinio kibernetinio saugumo centro švietimo veiklų planas Nr. 52K-1, kuriame įvardinti vykdomų mokymų pavadinimai, suteikti prioritetai, nurodytas finansavimas, datos, tikslai, tikslinės grupės, planuojamas dalyvių skaičius, kompetencijos, kurios stiprinamos, atsakingi vykdytojai, veiklos vertinimo rodikliai. Taip pat, 2023-03-06 įsakymu Nr. V-180 "Dėl Lietuvos respublikos krašto apsaugos ministro valdymo sričių 2023–2025 metų strateginio veiklos plano patvirtinimo" patvirtintame plane numatyta įgyvendinti projektą „Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų dirbantiesiems“ ir tęsti švietėjišką veiklą, organizuojant bazinius ir higienos kibernetinio saugumo mokymus.			
3 priemonė: Parengti ir patvirtinti tipinį kibernetinių incidentų valdymo planą.	2023-06-30	Įgyvendinta	Vėlavo
Atsakingi subjektai: Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos; Lietuvos Respublikos krašto apsaugos ministerija			

„KIBERNETINIO SAUGUMO UŽTIKRINIMAS"

Valstybinio audito ataskaita: 2022-10-27 Nr. VAE-10

Rekomendacijų stebėsenos ataskaita

2026-09-09 13:24

Rekomendacija / priemonė	Iki kada turi būti įgyvendinta	Būklė	Laiko būklė
Rezultatas: Krašto apsaugos ministerijos 2023-10-16 įsakymu Nr. V-840 patvirtintas Tipinis kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planas. Nustatytos tipinės procedūros, atliekamos valdant kibernetinius incidentus ryšių ir informacinėse sistemose, susijusiose su ypatingos svarbos informacine infrastruktūra.			
4 priemonė: Patvirtinus tipinį kibernetinių incidentų valdymo planą, pateikti kibernetinio saugumo subjektams nurodymus įgyvendinti plano nuostatas ir įpareigoti juos ne vėliau kaip per 12 mėn. pasirengti kibernetinių incidentų valdymo planus.	2023-12-31	Įgyvendinta	Vėlavo
Atsakingas subjektas: Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos			
Rezultatas: Atnaujinus Nacionalinį kibernetinio incidentų valdymo planą (naujos redakcijos LRV nutarimas Nr. 818), jame pateiktas naujas tipinis incidentų valdymo procesas, pagal kurį subjektai per 12 mėn. nuo įtraukimo į Kibernetinio saugumo subjektų registrą, privalės pasitvirtinti savo kibernetinių incidentų valdymo planą. Šio plano tvirtinimas yra numatytas ir naujuosiuose kibernetinio saugumo reikalavimuose.			
5 priemonė: Nustatyti valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams prievolę dalyvauti nacionalinėse kibernetinio saugumo pratybose.	2024-12-31	Įgyvendinta	Laiku
Atsakingas subjektas: Lietuvos Respublikos krašto apsaugos ministerija			
Rezultatas: Naujos redakcijos Kibernetinio saugumo įstatymas (patvirtintas 2024-10-18) numato privalomus periodinius mokymus (jie gali būti ir pratybų forma) ne tik kibernetinio saugumo subjektų vadovams, bet ir visam personalui. Įstatymas taip pat numato pratybas Nacionalinio kibernetinio saugumo centro identifikuotiems asmenims, kurie bus pasitelkiami valdant kibernetines krizes.			
6 priemonė: Įvertinti galimybes įpareigoti ypatingos svarbos informacinės infrastruktūros valdytojus dalyvauti nacionalinėse kibernetinio saugumo pratybose.	2024-12-31	Įgyvendinta	Laiku
Atsakingas subjektas: Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos			
Rezultatas: Naujos redakcijos Kibernetinio saugumo įstatymas (patvirtintas 2024-10-18) numato privalomus periodinius mokymus (jie gali būti ir pratybų forma) ne tik kibernetinio saugumo subjektų vadovams, bet ir visam personalui. Įstatymas taip pat numato pratybas Nacionalinio kibernetinio saugumo centro identifikuotiems asmenims, kurie bus pasitelkiami valdant kibernetines krizes.			

Daugiau informacijos apie šio ir kitų auditų metu teiktas rekomendacijas ir jų įgyvendinimą rasite čia Atviri duomenys