Nacionalinio kibernetinių
incidentų valdymo plano
2 priedas

TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PROCESO APRAŠYMAS

Eil. Nr.	Veiksmo aprašymas	Dalyvis	Terminas	Rezultatas
Pradžia (nustatytas įvykis)				
1.	Įvertinti, ar tai kibernetinis incidentas. Gavus pranešimą apie įvykį arba jį nustačius, sprendžiama, ar jis galėtų būti laikomas kibernetiniu incidentu.	Kibernetinio saugumo subjekto saugumo operacijų centras (toliau – Kibernetinio saugumo subjekto SOC)	Kibernetinio saugumo subjekto kibernetinių incidentų valdymo plane nustatytais terminais.	Priimtas sprendimas, ar įvyko kibernetinis incidentas.
2.	Įvertinti kibernetinio incidento poveikį. Priėmus sprendimą, kad įvykis laikomas kibernetiniu incidentu, pagal Kibernetinio saugumo įstatyme ir Nacionaliniame kibernetinių incidentų valdymo plane (toliau – Planas) nustatytus kriterijus įvertinama, ar įvyko didelis kibernetinis incidentas.	Kibernetinio saugumo subjekto SOC	Ne vėliau kaip per 24 val. nuo įvykio registravimo.	Įvertintas kibernetinio incidento poveikis.
Pranešimas Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC)				
3.	Registruoti Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma). Nustačius, kad įvyko kibernetinis incidentas, apie tai informuojamas Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), Platformoje pateikiant Kibernetinio saugumo įstatyme numatytą informaciją.	Kibernetinio saugumo subjekto SOC	Ankstyvasis perspėjimas (apie didelį incidentą) – nedelsiant, bet ne vėliau kaip per 24 val. nuo sužinojimo. Pranešimas apie (nedidelį) kibernetinį incidentą –	Kibernetinis incidentas užregistruotas Platformoje.

			nedelsiant, bet ne vėliau kaip per 72 val. nuo sužinojimo.	
Kibernetinio incidento valdymas				
4.	Spręsti dėl kibernetinio saugumo priemonių taikymo. Užregistravus kibernetinį incidentą sprendžiama dėl tinkamiausių priemonių jam suvaldyti. Apie šias priemones informuojamas kibernetinio saugumo subjekto tinklų ir informacinių sistemų veiklą užtikrinantis padalinys arba jo funkcijas atliekantys asmenys (toliau – Kibernetinio saugumo subjekto IT)	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto kibernetinių incidentų valdymo plane nustatytais terminais.	Priimtas sprendimas dėl kibernetinio saugumo priemonių taikymo.
5.	Nustatyti, ar didelis kibernetinis incidentas. Vertinama, ar nedidelis kibernetinis incidentas netampa dideliu. Didelių kibernetinių incidentų pakartotinis vertinimas atliekamas tik patikslinant jo poveikį, nustatant pagrindinę priežastį, bet nekeičiant rūšies.	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto kibernetinių incidentų valdymo plane nustatytais terminais.	Įvertintas arba patikslintas kibernetinio incidento poveikis.
6.	Atnaujinti informaciją Platformoje. Nustačius, kad kibernetinis incidentas atitinka didelio kibernetinio incidento kriterijus, atnaujinama informacija pagal Kibernetinio saugumo įstatymo reikalavimus ir pateikiama tarpinė atitinkamų atnaujintų padėties	Kibernetinio saugumo subjekto SOC	Tarpinė ataskaita – NKSC nurodytais terminais. Pažangos ataskaita apie didelį kibernetinį incidentą – kas mėnesį, iki bus suvaldytas	Platformoje užregistruota tarpinė arba pažangos ataskaita.

	duomenų ataskaita (toliau – tarpinė ataskaita) arba pažangos ataskaita.		kibernetinis incidentas.	
7.	Įvertinti, ar reikalinga NKSC pagalba. Valdant didelį kibernetinį incidentą sprendžiama dėl turimų vidinių ir pasitelktų išorinių resursų pakankamumo kibernetiniam incidentui suvaldyti.	Kibernetinio saugumo subjekto SOC	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Įvertintos kibernetinio saugumo subjekto galimybės suvaldyti kibernetinį incidentą.
8.	Prašyti NKSC pagalbos. Nepavykstant didelio kibernetinio incidento suvaldyti turimais vidiniais ir pasitelktais išoriniais resursais, vertinamas poreikis kreiptis pagalbos į NKSC dėl kibernetinio incidento suvaldymo.	Kibernetinio saugumo subjekto SOC	Priėmus sprendimą kreiptis – nedelsiant.	Pateiktas pagalbos prašymas NKSC.
9.	Surinkti įrodymus. Valdant kibernetinius incidentus surenkami visi įrodymai, reikalingi pagrindinei kibernetinio incidento priežasčiai ar grėsmei nustatyti.	Kibernetinio saugumo subjekto IT	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Surinkti įrodymai.
10.	Taikyti kibernetinio saugumo priemones. Taikomos būtinos priemonės, kad būtų užkirstas kelias kibernetiniam incidentui plisti ar tęstis.	Kibernetinio saugumo subjekto IT	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Įgyvendinamas kibernetinio saugumo subjekto kibernetinio saugumo incidentų valdymo planas.
11.	Įvertinti, ar suvaldytas kibernetinis incidentas. Vertinamas taikomų techninių ir organizacinių priemonių veiksmingumas, ar kibernetinis incidentas tęsiasi, ar suvaldytas. Kibernetinio incidento	Kibernetinio saugumo subjekto SOC	Nuolat.	Priimtas sprendimas, ar kibernetinis incidentas suvaldytas.

	nesuvaldžius, toliau tęsiamas jo poveikio vertinimas ir techninių ir organizacinių priemonių taikymas.			
12.	Atkurti tinklų ir informacinių sistemų veiklą. Tinklų ir informacinių sistemų veikla atkuriama pagal jų veiklos atkūrimo planus.	Kibernetinio saugumo subjekto IT	Kibernetinio saugumo subjekto tinklų ir informacinių sistemų veiklos atkūrimo planuose nustatytais terminais.	Paslaugos kibernetinio saugumo subjekto tinklų ir informacinėmis sistemomis teikiamos įprastine tvarka ir terminais.
Kibernetinio incidento tyrimas				
13.	Atlikti kibernetinio incidento tyrimą. Suvaldžius kibernetinį incidentą, pagal surinktus įrodymus identifikuojama pagrindinė jį sukėlusi priežastis.	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto veiklos atkūrimo planuose nustatytais terminais.	Nustatyta pagrindinė kibernetinio incidento priežastis.
14.	Identifikuoti prevencines priemones. Nustačius pagrindinę priežastį, pateikiamos išvados ir rekomendacijos, kaip ateityje išvengti tokio pobūdžio kibernetinių incidentų.	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto veiklos atkūrimo planuose nustatytais terminais.	Pateiktos išvados ir rekomendacijos.
15.	Pateikti galutinę ataskaitą. Vadovaujantis Kibernetinio saugumo įstatymo ir Plano reikalavimais parengiama galutinė ataskaita ir registruojama Platformoje.	Kibernetinio saugumo subjekto SOC	Galutinė ataskaita – per 1 mėnesį nuo ankstyvojo perspėjimo (didelio kibernetinio incidento atveju), pranešimo apie kibernetinį incidentą gavimo	Platformoje užregistruota galutinė ataskaita.

			(nedidelio kibernetinio incidento atveju) arba nuo kibernetinio incidento suvaldymo.	

_____