Lietuvos Respublikos globalinės padėties nustatymo sistemos nuolatinių stočių tinklo veiklos tęstinumo valdymo plano
4 priedas

KIBERNETINIŲ INCIDENTŲ VALDYMO IR NACIONALINIO KIBERNETINIO SAUGUMO CENTRO INFORMAVIMO TVARKOS APRAŠAS

1. Kibernetinių incidentų valdymo ir Nacionalinio kibernetinio saugumo centro informavimo tvarkos aprašas (toliau – Aprašas) reglamentuoja kibernetinių incidentų valdymo ir Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – Centras) informavimo apie Lietuvos Respublikos globalinės padėties nustatymo sistemos nuolatinių stočių tinkle (toliau – LitPOS) įvykusius kibernetinius incidentus tvarką.

2. Centrui pranešama apie LitPOS įvykusius:

2.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo;

2.2. vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo;

2.3. nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

3. Pranešime apie didelio ir vidutinio poveikio kibernetinį incidentą nurodoma:

3.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionalinio kibernetinių incidentų valdymo plano, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nacionalinis kibernetinių incidentų valdymo planas), priede pateiktus kriterijus;

3.2. trumpas kibernetinio incidento apibūdinimas;

3.3. tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas;

3.4. kibernetinio incidento šalinimo tvarka (nurodoma, ar tai prioritetas, ar ne);

3.5. tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.

4. Centrui pateikiama kibernetinio incidento tyrimo ataskaita apie:

4.1. didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

4.2. vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

4.3. didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo.

5. Didelio ar vidutinio poveikio kibernetinio incidento vertinimo ataskaitoje nurodoma žinoma informacija:

5.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionalinio kibernetinių incidentų valdymo plano priede pateiktus kriterijus;

5.2. LitPOS, kuriame nustatytas kibernetinis incidentas, tipas (informacinė sistema, posistemė, elektroninių ryšių tinklas, tarnybinė stotis ir panašiai);

5.3. kibernetinio incidento veikimo trukmė;

5.4. kibernetinio incidento šaltinis;

5.5. kibernetinio incidento požymiai;

5.6. kibernetinio incidento veikimo metodas;

5.7. galimos ir (ar) nustatytos kibernetinio incidento pasekmės;

5.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

5.9. kibernetinio incidento būsena (aktyvus, pasyvus);

5.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

5.11. galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės;

5.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita remiantis Aprašo 4 punktu.

6. Didelio ar vidutinio poveikio kibernetinių incidentų tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis LitPOS ir (ar) atkuriama įprasta LiPOS veikla.

7. Ne vėliau kaip per aštuonias valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo LitPOS tvarkytojas informuoja LitPOS naudotojus, jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos LitPOS teikiamų paslaugų LitPOS naudotojams.

8. Apie kibernetinius incidentus Centras informuojamas naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės – Centro nurodytais kontaktais (tel. 1843; el. p. cert@nksc.lt).

9. LitPOS tvarkytojas imasi visų įmanomų priemonių, būtinų kibernetiniam incidentui suvaldyti ir LitPOS veiklai atkurti.

_____