**PRANEŠIMAS**

**APIE KIBERNETINĮ INCIDENTĄ**

Data Nr. Numeris

Sudarymo vieta

|  |  |
| --- | --- |
| **Kontaktinė informacija** | Juridinis asmuo (įmonė): spustelėkite čia norėdami įvesti tekstą |
| Adresas: spustelėkite čia norėdami įvesti tekstą |
| Telefonas, el. paštas: spustelėkite čia norėdami įvesti tekstą |
| Informaciją apie kibernetinį incidentą pateikiančio asmens vardas, pavardė:  spustelėkite čia norėdami įvesti tekstą |
| Pareigos: spustelėkite čia norėdami įvesti tekstą |
| Telefonas, el. pašto adresas: spustelėkite čia norėdami įvesti tekstą |
| **Kibernetinio incidento apibūdinimas** | **Kibernetinio incidento grupė:**  Pasirinkite grupę1 |
| Tiksli data, laikas ir fizinė vieta, kada ir kur kibernetinis incidentas įvyko ir nustatytas:  spustelėkite čia norėdami įvesti tekstą |
| Trumpas kibernetinio incidento apibūdinimas (nurodyti kiek įmanoma tikslesnę informaciją):  spustelėkite čia norėdami įvesti tekstą |
| Kibernetinio incidento statusas:   |  |  | | --- | --- | |  | Suvaldytas | |  | Nesuvaldytas | |  | Dalinai suvaldytas | |
| **Kibernetinio incidento reikšmė:**   |  |  | | --- | --- | |  | didelio poveikio kibernetinis incidentas | |  | vidutinio poveikio kibernetinis incidentas | |  | mažo poveikio kibernetinis incidentas | |
| **Kibernetinio incidento poveikis:**  gali turėti neigiamos įtakos ypatingos svarbos informacinių ir ryšių technologijų sistemoms bei duomenims  gali turėti nusikalstomos veikos požymių  gali būti susijęs su asmens duomenų saugumo pažeidimais |
| **Kibernetinio incidento šalinimo tvarka (veiksmai ir priemonės)** | spustelėkite čia norėdami įvesti tekstą |
| **Kita svarbi informacija** | spustelėkite čia norėdami įvesti tekstą |

Paaiškinimai:

1 kibernetinių incidentų pavyzdžiai:

|  |  |
| --- | --- |
| 1. | * Nepageidaujami laiškai ir (ar) klaidinančios, žeidžiančios informacijos platinimas trikdo ypatingos svarbos informacinių ir ryšių technologijų sistemų ar duomenų veiklą ir (ar) teikiamas paslaugas |
| 2. | * Aptikta moderni kenkimo programinė įranga (angl. advanced persistent threat, APT) * Ypatingos svarbos informacinių ir ryšių technologijų sistemos ar duomenys aktyviai kontroliuojami įsibrovėlių (pavyzdžiui, „galinės durys“ (angl. back door), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. Botnet) infrastruktūros dalimi) * Kenkimo programinė įranga, trikdanti saugumo priemonių darbą * Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja * Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus |
| 3. | * Ypatingos svarbos informacinių ir ryšių technologijų sistemų ar duomenų paketų / informacijos perėmimas * Ypatingos svarbos informacinių ir ryšių technologijų sistemų ar duomenų klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant socialinės inžinerijos principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus * Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti) |
| 4. | * Išnaudojamas vienas ar keli nežinomi (angl. zero day) pažeidžiamumai, siekiant tikslingai sutrikdyti konkrečią ypatingos svarbos informacinių ir ryšių technologijų sistemą ar duomenis * Išnaudojamas vienas ar keli nežinomi (angl. zero day) pažeidžiamumai * Vidinė ypatingos svarbos informacinių ir ryšių technologijų sistemų ar duomenų žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita) * Išnaudojami žinomi ir viešai publikuoti pažeidžiamumai arba atliekami bandymai prisijungti prie ypatingos svarbos informacinių ir ryšių technologijų sistemų ar duomenų parenkant slaptažodžius |
| 5. | * Veiksmai prieš ypatingos svarbos informacinių ir ryšių technologijų sistemą ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, ypatingos svarbos informacinių ir ryšių technologijų sistemos ar jos dalies pažeidimas, sutrikdantis ypatingos svarbos informacinių ir ryšių technologijų sistemos teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui * Gaunama neteisėta prieiga prie ypatingos svarbos informacinių ir ryšių technologijų sistemos, duomenų, taikomosios programinės įrangos ar paslaugos |
| 6. | * Teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas * Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui * Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui |
| 7. | * Neteisėta prieiga prie informacijos, galinčios turėti įtakos ypatingos svarbos informacinių ir ryšių technologijų sistemos veiklai ir (ar) teikiamoms paslaugoms * Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas * Neteisėta įtaka ypatingos svarbos informacinių ir ryšių technologijų sistemos veiklai ir (ar) teikiamoms paslaugoms |
| 8. | * Kiti incidentai |