

KIBERNETINĖS ATAKOS VALDYMO PLANAS

Šis dokumentas yra šablonas, skirtas padėti organizacijoms pasirengti kibernetinėms atakoms ir efektyviai jas valdyti. Kiekviena organizacija turėtų pritaikyti šį planą pagal savo specifinius poreikius.

The logo consists of the lowercase letters 'no' and the uppercase letters 'IT' in a bold, white, sans-serif font, set against a solid red rectangular background.

noIT

Kibernetinio Saugumo Sprendimai

1. ORGANIZACIJOS INFORMACIJA

- **Organizacijos pavadinimas:** [Irašykite savo organizacijos pavadinimą]
 - **Atsakingas asmuo už saugumą:** [Vardas, pareigos, kontaktai]
 - **Incidentų valdymo komanda:** [Sąrašas su kontaktine informacija]
 - **Kritinių sistemų sąrašas:** [Išvardykite svarbiausias IT sistemas]
-

2. KIBERNETINĖS ATAKOS NUSTATYMAS IR PIRMINĖ REAKCIJA

2.1 Atakos atpažinimas

- Stebėjimo sistemų signalų analizė.
- Įtartinų veiklų identifikavimas ir klasifikavimas.
- Skubus informavimas atsakingiems asmenims.

2.2 Sistemos izoliavimas ir žalos ribojimas

- Pažeistų sistemų atjungimas nuo tinklo.
- Prieigos kontrolės peržiūra.
- Kenkėjiškos veiklos neutralizavimas.

2.3 Darbuotojų budrumas ir veiksmų gairės

- Jei darbuotojas netyčia paspaudžia ant įtartinos nuorodos ar prisegto failo:
 - Nedelsiant informuoti informacinių technologijų skyrių.
 - Neatidaryti papildomų nuorodų ar failų.
 - Jei reikalinga, atjungti kompiuterį nuo tinklo.
 - Pranešti atsakingam už kibernetinį saugumą asmeniui.

3. DUOMENŲ APSAUGA IR SISTEMŲ ATKŪRIMAS

3.1 Atsarginių kopijų tikrinimas ir atkūrimas

- Atsarginių kopijų prieinamumo patikra.
- Kritinių sistemų atkūrimo procedūros.

3.2 Sistemos atkūrimo tvarka

1. Pagrindinių sistemų atkūrimas.
2. Tinklų ir ryšio atstatymas.
3. Darbo vietų atstatymas.
4. Klientų ir darbuotojų informavimas.

4. KIBERNETINĖS ATAKOS ANALIZĖ IR ATEITIES PREVENCIJA

4.1 Incidento tyrimas

- Atakos šaltinio analizė.
- Sistemos žurnalų ir įrodymų rinkimas.
- Incidentų registravimo registras (visi incidentai turi būti registruojami, net ir smulkūs pažeidimai).

4.2 Prevencinės priemonės

- Saugumo atnaujinimai ir pakeitimai.
- Prieigos valdymo ir autentifikacijos sustiprinimas.
- Darbuotojų mokymai.

5. KOMUNIKACIJOS PLANAS

5.1 Vidaus komunikacija

- Atsakingų asmenų sušaukimas.
- Vadovybės ir IT skyriaus informavimas.

5.2 Išorinė komunikacija

- Klientų ir partnerių informavimas.
- Bendradarbiavimas su teisėsauga.
- Viešųjų ryšių strategija.
- Incidentų pranešimas Nacionaliniam kibernetinio saugumo centrui (NKSC) pagal teisės aktų reikalavimus.

6. TESTAVIMAS IR NUOLATINIS TOBULINIMAS

6.1 Reagavimo į incidentus testavimas

- Periodinės pratybos ir testavimas.
- Kibernetinių atakų simuliacijos.

6.2 Plano peržiūra ir atnaujinimas

- Reguliarūs patikrinimai ir atnaujinimai.
- Incidentų analizės išvadų įtraukimas.

Pastaba: Šis dokumentas yra šablonas. Jis turėtų būti individualiai pritaikytas pagal organizacijos specifinius poreikius ir reguliariai atnaujinamas atsižvelgiant į naujas kibernetines grėsmes.

<https://www.noit.lt/>