PATVIRTINTA
Šilalės rajono savivaldybės
priešgaisrinės tarnybos viršininko
2023 m. liepos 18 d. įsakymu Nr. P1-
12

KIBERNETINIO SAUGUMO ŠILALĖS RAJONO SAVIVALDYBĖS PRIEŠGAISRINĖJE TARNYBOJE POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

Šilalės rajono savivaldybės priešgaisrinės tarnybos (toliau – Priešgaisrinė tarnyba) kibernetinis saugumas, dar vadinamas skaitmeniniu saugumu, yra skaitmeninės informacijos, įrenginių ir išteklių apsaugos praktika. Tai apima tarnybos asmeninę informaciją, paskyras, failus, nuotraukas ir pinigus. Pagrindinis tikslas – efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes, užtikrinti saugų naudojimąsi informacinių ir ryšių technologijų teikiamomis galimybėmis.

Pagrindinės sąvokos:

1. **Kibernetinė erdvė** – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija.
2. **Kibernetinis incidentas** – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.
3. **Kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.
4. **Kibernetinių incidentų valdymas** – procedūros, kurių tikslas – aptikti, analizuoti kibernetinius incidentus ir reaguoti į juos, taip pat atkurti įprastinę ryšių ir informacinių sistemų veiklą.

II SKYRIUS
KIBERNETINIO SAUGUMO PRINCIPAI

Kibernetinis saugumas grindžiamas šiais kibernetinio saugumo principais:

5. kibernetinės erdvės nediskriminavimo – Priešgaisrinės tarnybos informacija yra saugoma vienodai tiek fizinėje, tiek kibernetinėje erdvėje;
6. kibernetinio saugumo rizikos valdymo – taikomos priemonės turi užtikrinti Priešgaisrinės tarnybos rizikos suvaldymą;
7. kibernetinio saugumo proporcingumo –kibernetinio saugumo priemonės neturi apriboti Priešgaisrinės tarnybos veiklos kibernetinėje erdvėje labiau, negu tai būtina;
8. viešojo intereso viršenybės – taikomos kibernetinio saugumo priemonės turi užtikrinti Priešgaisrinės tarnybos apsaugą, tačiau neturi pažeisti vartotojų teisių ar apriboti jų laisvės kibernetinėje erdvėje;
9. standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo priemones, vadovaujamasi nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir

informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

III SKYRIUS
PAGRINDINĖS KIBERNETINIO SAUGUMO GRĖSMĖS IR ŠALTINIAI

10. Priešgaisrinės tarnybos duomenų nutekinimas/vagystė;
11. Duomenų, informacijos sunaikinimas;
12. Sugadinti technologiniai įrenginiai;
13. Išpirkos reikalaujančios kenkėjiškos programos;
14. Kenkėjiškos programos, įvairių tipų virusai, šnipinėjimo programos;
15. Pasinaudojimas žmogiškosiomis klaidomis informacijai išgauti, įskaitant sukčiavimą el. paštu ir tekstinėmis žinutėmis;
16. Dezinformacija, kai naudojant išmaniąją vaizdo klastotę ir robotus, apsimetama kitu asmeniu ir platinama netinkamo pobūdžio informacija.

Galimi kibernetinių atakų šaltiniai:

17. Nedraugiškos valstybės: renka informaciją apie mūsų Valstybei svarbias paslaugas, veiklas, kad sutrikdytų jų veiklą;
18. profesionalūs nusikaltėliai: kibernetines atakas rengia siekdami finansinės naudos, dėl politinių tikslų;
19. pavieniai nusikaltėliai: kibernetines atakas rengia siekdami finansinės naudos, dėl politinių tikslų ar norėdami išbandyti savo jėgas;
20. darbuotojai: esami ar buvę darbuotojai, turintys asmeninių nuoskaudų, nepatenkinti darbo santykiais ar turintys kitų motyvų.

IV SKYRIUS
PAREIGOS UŽTIKRINANT KIBERNETINĮ SAUGUMĄ

21. Priešgaisrinė tarnyba atsako už valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams;
22. atlieka rizikos vertinimą ir, esant būtinybei, įdiegia kitas, technines ir organizacines kibernetinio saugumo priemones;
23. įvertinus kibernetinio incidento dydį, praneša atitinkamoms institucijoms (Šilalės rajono savivaldybei, Nacionalinio kibernetinio saugumo centrui arba policijai) apie ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones;
24. paskiria kompetentingą asmenį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą;
25. Nuolat daryti atsargines dokumentų kopijas;
26. Neatidarinėti įtartinų elektroninių laiškų ar elektroniniuose laiškuose atsiųstų neaiškių nuorodų;
27. Nenaudoti populiarių slaptažodžių, slaptažodžius kurkite su įvairiais simboliais;
28. Nenaudoti identiškų slaptažodžių skirtingoms paskyroms;
29. Prisijungimo slaptažodžius sugalvoti unikalius, ne trumpesnius kaip 10 simbolių;
30. Nepalikti prisijungimo duomenų, slaptažodžių gerai matomoje darbo vietoje;
31. Neprijungti nežinomų USB atmintinių prie Priešgaisrinės tarnybos įrenginių;
32. Neatskleisti prisijungimo duomenų slaptažodžių tretiesiems asmenims;
33. Baigus darbą visuomet atsijunkite nuo prisijungtos programos, neuždarinėkite langų neatsijungus;

34. Periodiškai atnaujinkite programinę įrangą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

35. Kibernetinio saugumo politika keičiama ir tvirtinama Priešgaisrinės tarnybos viršininko įsakymu;

36. Su kibernetinio saugumo politika supažindinti visus darbuotojus;

37. Kibernetinio saugumo politika peržiūrima ne rečiau kaip kas du metus;

38. Kibernetinė politika yra skelbiama viešai, Priešgaisrinės tarnybos internetinėje svetainėje www.sspt.lt

---