Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Vilniaus universitetas

SISTEMINIŲ ŽURNALŲ TERMINUOTO SAUGOJIMO PASLAUGA

Kompiuterių tinklo sisteminės informacijos saugojimo politika (taisyklės)

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Vilnius

2018

Sisteminių žurnalų terminuoto saugojimo paslauga
Kompiuterių tinklo sisteminės informacijos saugojimo politika (taisyklės)

1. Bendrosios nuostatos:
   1.1. Kompiuterių tinklo sisteminės informacijos saugojimo politika (toliau – POLITIKA) nustatyta vadovaujantis Lietuvos Respublikos teisės aktais bei ES direktyvomis:
      1.1.1.1. LR kibernetinio saugumo įstatymas [TAR, 2014-12-23, Nr. 20553];
      1.1.1.2. LR elektroninių ryšių įstatymas [Valstybės žinios, 2004-04-30, Nr. 69-2382];
      1.1.1.3. LR valstybės ir tarnybos paslapčių įstatymas [Valstybės žinios, 1999-12-08, Nr. 105-3019].
      1.1.1.4. LRV nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo [TAR, 2018-08-20, Nr. 13252]
      1.1.1.5. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti [https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016L1148&from=LT]
      1.1.1.6. LR vidaus reikalų ministerija. Rekomendacijos kibernetiniam saugumui užtikrinti [https://vrm.lrv.lt/lt/veiklos-sritys/rekomendacijos-kibernetiniam-saugumui-uztikrinti]
      1.1.1.7. LITNET tinklo naudojimo taisyklės [https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.405853]
   1.2. Ši POLITIKA yra privaloma LITNET programoje dalyvaujančioms, LITNET paslaugas naudojančioms institucijoms.
2. Pagrindinės sąvokos:
   2.1. Kompiuterių tinklo sisteminės informacijos surinkimas - tai įvykių registravimas sisteminiuose žurnaluose.
   2.2. Kompiuterių tinklo sisteminės informacijos saugojimas – sisteminių žurnalų saugojimas nuo pakeitimų bei nesankcionuotos prieigos.
   2.3. Kompiuterių tinklo įrenginio (toliau – įrenginio) administratorius – asmuo, atsakingas už įrenginio tinkamą veikimą ir naudojimą.
3. Tikslas:
   3.1. Kompiuterių tinklo sisteminė informacija (*angl*. logs) yra svarbi užtikrinant tinkamą institucijos kompiuterių tinklo valdymą, kibernetinę saugą, operatyvų kilusių incidentų sprendimą, grėsmių aptikimą.
   3.2. Įvykių registravimo sisteminiuose žurnaluose tikslas – kaupti informaciją įvykių auditui ir kontrolei, siekiant laiku ir operatyviai reaguoti į incidentus; išsiaiškinti pažeidžiamumus; užkirsti kelią tolesniems piktavališkiems veiksmams bei išaiškinti pažeidėjus.
   3.3. Sisteminės informacijos saugojimo tikslas – užtikrinti registruotų įvykių informacijos integralumą, nekeičiamumą ir pasiekiamumą nustatytu terminu.
4. Kompiuterių tinklo sisteminės informacijos surinkimui ir saugojimui taikomi šie pagrindiniai principai:
   4.1. skaidrumo. Šis principas reiškia, kad surinkta bei saugoma sisteminė informacija yra teikiama tik tiems asmenims, kurie pagal teisės aktus turi teisę šią informaciją gauti;
   4.2. sąžiningumo. Šis principas reiškia, kad sisteminė informacija renkama, saugoma ir valdoma nesiimant apgaulės, sukčiavimo ir vengiant nesąžiningų veiksmų;
   4.3. bendradarbiavimo. Šis principas reiškia, kad bet kokie santykiai tarp kompiuterių tinklo įrangos administratorių bei už sisteminės informacijos saugojimą ir valdymą atsakingų asmenų grindžiami abipusio geranoriškumo kriterijais;
   4.4. pagarbos. Šis principas reiškia, kad kompiuterių tinklo įrangos administratorių bei už

sisteminės informacijos saugojimą ir valdymą atsakingų asmenys visuomet elgiasi pagarbiai vieni kitų bei kitų suinteresuotų asmenų atžvilgiu;

4.5. kokybės. Šis principas reiškia, kad sisteminės informacijos surinkimo ir saugojimo veikla turi būti nuolat vertinama ir tobulinama atsižvelgiant į poreikius ir praktikoje priimtinus bei naudotinus saugumo standartus;

4.6. konfidencialumo. Šis principas reiškia, kad visa surinkta bei saugoma sisteminė informacija yra naudojama tik teisėtais tikslais;

4.7. nekomercinio naudojimo. Šis principas reiškia, kad surenkama bei saugoma sisteminė informacija negali būti naudojama siekiant komercinių tikslų;

4.8. teisių ir pareigų vienybės. Šis principas reiškia, kad bet kokios su Sisteminės informacijos surinkimu bei saugojimu susijusios teisės nėra absoliučios ir yra neatsiejamos nuo LITNET tinklo naudojimo taisyklėse numatytų pareigų.

5. Įvykių registravimas sisteminiuose žurnaluose:
   5.1. Kiekvienas kompiuterių tinkle veikiantis įrenginys turi turėti administratorių.
   5.2. Turi būti užtikrintas nuolatinis kompiuterių tinkle esančių įrenginių veiklos įvykių registravimas realiu laiku.
   5.3. Kompiuterių tinklo įrangos laikrodžiai, pagal kuriuos nustatomas įvykių laikas, turi būti automatiškai sinchronizuojami su internetiniais laikrodžiais [NTP servisais].
   5.4. Įvykiai turi būti registruojami kiekvieno įrenginio standartiniu formatu. Papildomai įvykiai gali būti registruojami ir specialius poreikius atitinkančiu formatu.
   5.5. Įvykiai turi būti registruojami vidiniame ir nutolusiame sisteminiuose žurnaluose.
   5.6. Įvykių žurnaluose turi būti registruojami:
      5.6.1. įvykio tikslus laikas ir data;
      5.6.2. įvykio rūšis ir pobūdis (naudotojų, procesų, sistemų, tinklo ir kt.);
      5.6.3. įvykio turinys, rezultatas;
      5.6.4. kiti kibernetinei saugai ir įrenginių veikimo bei naudojimo auditui svarbūs įvykiai.
   5.7. Įvykių žurnaluose turi būti užtikrintas registravimas sėkmingų ir nesėkmingų bandymų prisijungti prie tinklo įrenginių bei sistemų..
   5.8. Vadovaujantis rizikos analize įvykių sąrašas gali būti papildytas.
   5.9. Reikalaujamų registruoti įvykių sąrašas formuojamas pagal LR teisės aktus, derinamas LITNET ekspertų bei LITNET CERT grupėse
6. Reikalavimai sisteminės informacijos saugojimui:
   6.1. Sisteminiai žurnalai turi būti saugomi Lietuvos Respublikos teritorijoje;
   6.2. Sisteminiai žurnalai turi būti saugomi ne trumpiau kaip 6 mėnesius. Saugojimo terminas turi atitikti LR įstatymų ir ES Direktyvų nustatytus reikalavimus;
   6.3. Turi būti užtikrintas įvykių žurnalų saugojimas nuo įsilaužimo, neautorizuotos prieigos, įvykių klastojimo ir trynimo;
   6.4. Prieiga prie nutolusių sisteminių žurnalų turi būti registruojama.
   6.5. Visą įvykių žurnalų saugojimo laiką turi būti galimybė nustatyti su įvykiais susijusius asmenis bei sistemas.
7. Privalomas periodinis įvykių žurnalų peržiūrėjimas (ne rečiau nei kartą per mėnesį).
8. LITNET paslaugas naudojančioms institucijoms, patenkančioms į LRV patvirtintą YSII objektų sąrašą, taikomi reikalavimai, išvardinti LR Vyriausybės patvirtintame organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše.