LOKSA LINNAPEA

KÄSKKIRI

Loksal 20. jaanuar 2014 nr 3

Loksa Linnavalitsuse võrguliikluse monitooringu korra kinnitamine

Võttes aluseks kohaliku omavalitsuse korralduse seaduse § 50 lg 1 p 3 ja arvestades Vabariigi Valitsuse 20.12.2007 määruses nr 252 „Infosüsteemide turvameetmete süsteem“ sätestatut, annan alljärgneva

k ä s k k i r j a:

1. Kinnitada Loksa Linnavalitsuse võrguliikluse monitooringu kord vastavalt lisale.

2. IT-spetsialist Ain Kasetalul teha Loksa Linnavalitsuse võrguliikluse monitooringu kord allkirja vastu teatavaks Loksa Linnavalitsuse teenistujatele.

3. Käskkirja on võimalik vaidlustada Tallinna Halduskohtus (Pärnu mnt 7, Tallinn 15082) 30 päeva jooksul arvates teatavakstegemisest.

Värner Lootsmann
linnapea

KINNITATUD
Loksa linnapea 20.01.2014 käskkirjaga nr 3
„Loksa Linnavalitsuse võrguliikluse monitooringu korra kinnitamine"
LISA

Võrguliikluse monitooringu kord

1. Eesmärk

Käesolev dokument annab suunised võrguliiklus monitooringu süsteemi OSSIM tulemite kasutamiseks turvaintsidentide lahendamisel Harjumaa omavalitsuste liidus.

Monitooringusüsteem OSSIM annab kehtestatud reeglistiku alusel informatsiooni lokaalvõrgus toimuvast s.t selle eesmärgiks on teenistujate käsutuses olevate arvutite, serverite, võrguseadmete ja muu arvutitehnika seire, eesmärgiga saada ülevaade linnavalitsuse võrgus toimuvast ning avastamaks võimalikke sisemistest või välimistest põhjustest tekkivate kõrvalekaldeid. Samuti on monitooringu eesmärgiks ka pahatahtliku võrguliikluse (näiteks viirused või ründed) tuvastamine ning tõkestamine.

2. Määrangud

Turvaintsidentideks loetakse muuhulgas järgmisi sündmusi:

1) OSSIM poolt registreeritud sündmus, millele on reeglite järgi omistatud riski tase, milleks võivad olla süsteemi tõrked, töö katkemine või seadme rike;
2) vaatlusega avastatavad intsidendid nt inimlikud vead, juurdepääsu väärkasutused, lubamatud muudatused süsteemis, füüsiliste turvameetmete rikkumine.

3. Tegevused

Linnavalitsuse teenistujad peavad viivitamatult teavitama turvaintsidendist või selle kahtlustest linnapead ja IT-spetsialisti telefoni või e-posti teel. Intsident või selle oht tuleb kirjeldada võimalikult täpselt.

IT-spetsialist määrab turvaintsidendile lahendamise prioriteedi (kõrge, keskmine, madal). Linnapea võib prioriteeti muuta.

Sõltuvalt turbeastmest on tegutsemisjuhised järgmised:

1) Madal risk – IT-spetsialist korraldab intsidendi lahendamise, kirjutab lahendamisejärgselt raporti, mille edastab linnapeale;
2) Keskmine risk - IT-spetsialist korraldab intsidendi lahendamise. Pärast turvaintsidendi lahendamist kirjutab IT-spetsialist raporti ja edastab selle linnapeale ja HOL juhatajale.
3) Kõrge risk - IT-spetsialist teavitab intsidendist koheselt CERT-EEd vastavalt ISKE rakendusjuhendis sätestatud nõuetele. IT-spetsialist korraldab intsidendi lahendamise. Pärast turvaintsidendi lahendamist kirjutab IT-spetsialist raporti ja edastab linnapeale.

Kõrge riskiga intsidentide puhul informeerib linnapea vajadusel koostööpartnereid ning vajadusel kuulutab välja hädaolukorra.

IT-spetsialist jagab kasutajatele juhtnööre vältimaks ja piiramaks võimalikke ja tekkinud kahjusid.

Intsident loetakse lõpetatuks, kui on kasutusele võetud asjakohased meetmed kahjude ärahoidmiseks, koostatud raport, hinnatud kahjud ning vajadusel teavitatud CERT-EEd,

täiendatud OSSIM seire reeglistikku, rakendatud infotehnoloogilised meetmed ja koolitatud personali.

4. Muudatused

Võrguliikluse monitooringu korra tõhusust hinnatakse kord aastas. Pidevalt täiendatakse intsidentide seire reegleid ning hinnatakse neid pärast iga kõrge riskiga intsidenti, kui lahendamisel leiti korras puudusi.

5. Õppetunnid

Intsidentide lahendite raportite alusel on soovitatav linnapeal koos IT-spetsialisti ja IT turvalisuse ekspertidega koostada õppematerjale ning neid kasutada linnavalitsuse teenistujate ning laiema üldsuse koolitamiseks turvalisuse alal.