**Algatamise eest vastutavad:** ametiasutuse/ettevõtte juhtkond, IT-turvaosakond  
**Rakendamise eest vastutavad:** IT-turvaosakond  
  
**ISKE Kataloog:** Versioon 8.06  
**ISKE Meede:**  M 2.299

Turvalüüsi (tulemüüri) turvapoliitika  
KOV võrkude seadistamisel

Kohalike omavalitsuste võrkude seadistamisel tuleb olulist rõhku panna tulemüüri seadistamisele. Tulemüüridel on täitev roll võrgu turvalisuse tagamisel ning eriti oluline on tagada nende turvaline ja nõuetekohane käitamine

1. **Ligipääs ja haldamine**
   1. Tulemüüride seadistamiseks ning haldamiseks peab olema eraldatud administreerimise võrk, kasutades VLAN-e. Samuti peab olema võimalik tulemüüre seadistada ka läbi krüpteeritud ühenduse. Auditeerijad peavad saama kasutada samu liideseid.
   2. KOV-i tulemüüri seadmeid võib hallata ainult IT-teenusepakkuja poolne võrguadministraator. Võrguadministraatorite lisandumisel, kes ei ole IT-teenusepakkuja töötajad, tuleb ligipääsud KOV-ga eraldi kokku leppida.
   3. Tulemüüri seadmetele füüsiline ligipääs peab olema reguleeritud KOV-i ja IT-teenusepakkuja vahelises lepingus ning KOV-i sisekorraeeskirjade reeglitega. Ligipääs tohib olla ainult IT-teenusepakkujal või kooskõlastatult IT-teenusepakkujaga kolmandatael osapooltel (nt ISP hooldustööd vms).
   4. Seadmete konsoolporti tuleb kasutada ainult hädaolukordades, kus enam läbi turvaliste ühenduste seadmele ligipääsu ei ole või kui administreerimise liides on tõrkeolekus.
2. **Turvalisus ja seadistamine**
   1. Tulemüüride seadistamisel peab olema jälgitud põhimõtet – kõik mis pole lubatud, on keelatud. Sellise põhimõtte jälgimine tagab võimalikult turvalise ning kontrollitud tulemüüri.
   2. Seadistamisel kasutatud turvavõtmed peavad olema tulemüüri seadme peal krüpteeritud kujul. Samuti peab olema krüpteeritud kujul tulemüüri konfiguratsioonifail.
   3. Tulemüüri reeglite seadistamisel tuleb veenduda reegli turvalisuses – vajadusel kasutada nelja silma printsiipi. Samuti tuleks kasutada ACL-e, et haldus oleks lihtsamini jälgitav ning uute reeglite lisamine oleks kasutajasõbralikum.
   4. Esmapaigaldamisel tuleb ära eemaldada kõik vaikeseaded ja väärtused. Samuti tuleb esimese sammuna paika seadistada turvaline ligipääs tulemüüriseadmele.
   5. Tulemüüris olevad reeglid peavad olema seadme peal kommenteeritud. Reegli kommentaar peab olema võimalikult lakooniline.
3. **Logid ja hooldus**
   1. Tulemüüri seadistamisel peab olema võimalik logisid jälgida. Logid tuleb hoida seadme peal või krüpteeritud kujul välisel andmekandjal või eraldi logiserveris.
   2. Tulemüüri puhul peab logima kõiki võimalikke sündmusi. Eriti tähtsad on konfiguratsiooni puudutavad logid ning seadme pihta tulevate ühenduste logid (võimalik rünnakud).
   3. Logide analüüsimine peab olema korrapärane, kuid mitte vähem kui kord kuus.
   4. Tulemüüri seadet peab hoidma alati nii tarkvara kui ka püsivara uuenduste puhul kõige värskema ja turvalisema versiooni peal. Samuti tuleb jälgida seda, et alati pole kõige värskem uuendus kõige turvalisem. Võimalusel kasutada pikalt testitud ning tootja poolt kõige turvalisemaks märgitud tarkvara versiooni.
   5. Seadmete soetamisel ning väljavahetamisel tuleb jälgida, et antud tulemüüri seade sobituks kokku olemasolevasse võrguhaldusesse. Võimalusel tuleks valida sellise tootja seadmed, mis omavahel hästi kokku integreeruks. Samuti peab uus seade vastama kõikidele tänapäevastele turvakriteeriumitele.
4. **Andmevarundus ja rikked**
   1. Tulemüüri konfiguratsioonifaili peab regulaarselt varundama. Varukoopiat tuleks hoida krüpteeritult või parooliga kaitstud keskkonnas. Tulemüüri konfiguratsioonist tuleb teha alati koopia ka siis, kui tehtud on mingi suurem muudatus.
   2. Tulemüüri konfiguratsiooni rikke korral peab jääma alati turvalisuse olukord selliseks, et väljaspool turvalisi administreerimise liideseid ligipääs puudub. Rikkele peab reageerima esimesel võimalusel või vastavalt turvaastmele.
   3. Võimalikest turvaintsidentidest tuleb teavitada koheselt IT-teenusepakkujat ning võrguadministraatorit.
5. **Dokumenteerimine**
   1. Tulemüüri konfiguratsiooni muudatusi peab dokumenteerima IT-teenusepakkuja, kasutades selleks vastavaid tarkvaralisi lahendusi, mille abil on võimalik tuvastusi toimunud muudatusi.
   2. Loodud dokumentatsioon peab olema lihtsasti arusaadav. Näiteks peab olema võimalik seda kasutada võimalike rikete tuvastamiseks, mis on tekkinud seadistamise käigus.