**Algatamise eest vastutavad:** IT-juht, infoturbeosakond  
**Rakendamise eest vastutavad:** administraator  
  
**ISKE Kataloog:** Versioon 8.06  
**ISKE Meede:**  M 6.94

Turvalüüside hädaolukorraks valmisoleku plaan  
KOV võrkudes

Turvalüüsidel (edaspidi tulemüür) on võrguühenduse käideldavuse osas väga oluline roll. Tulemüüris esinevate tõrgete korral võivad olla rasked tagajärjed.

1. **Monitooring ja logimine**
   1. Tulemüüri logimine ja monitooring on oluline samm, et ennetada võimalikke hädaolukordasid.   
      Selle jaoks peab olema võimalik tuvastada logidest võimalikke konfiguratsiooni vigasid ning tulemüüri pihta tulevaid rünnakuid.
   2. Tõhususe suurendamiseks peab olema võimalik automaatselt tuvastada tulemüüri pihta tulevaid rünnakuid. Lisaks peab olema võimalik tuvastada KOV-s kasutavate võrgusüsteemide pihta tehtuid ebaõnnestunud sisselogimiskatseid.
   3. Hädaolukorra ennetamiseks peab olema võimalik monitoorida tulemüüriseadmete töökeskkonna nõuete vastavust seadmete tootja poolt ettenähtud parameetrite suhtes (nt temperatuur, õhuniiskus). Kui seadmete töökeskkonna parameetrid väljuvad tootja poolt ette antud vahemikest, siis peab toimuma automaatne IT-teenusepakkuja teavitamine. Töökeskkonna parameetrite kriitilise piiri ületamise korral peab toimuma seadmete automaatne väljalülitus.
   4. IT-teenusepakkuja peab kasutama tarkvaralisi monitooringu lahendusi tulemüüriseadme staatuse jälgimiseks.
2. **Diagnostika ja konfiguratsioon**
   1. Tulemüüris peab olema võimalus võimalikult lihtsasti ja kasutajasõbralikult näha jookvat konfiguratsiooni. Jooksva konfiguratsiooni lugemisel peab olema tuvastatav ( kommentaaride abil) iga reeglit funktsionaalsus ja eesmärk.
   2. Tulemüüri konfiguratsioonis peab valmis olema tehtud reeglid turvaintsidendi või hädaolukorra piiramiseks. Enamasti hõlmab see kõikide (va tööks hädavajalikud) portide kinni panemist ning maksimaalset liikluse filtreerimist.
   3. Ründe tuvastamiseks ning blokeerimiseks peab kasutama IDS ja IPS süsteeme.
   4. Tulemüüri peab olema võimalik ka analüüsida riistvara näitajate poolest. See aitab ennetada seadme võimalikku füüsilist riket. Seadme füüsilise rikke korral tuleb seade välja vahetada esimesel võimalusel või vastavalt turbeastmele.
   5. Tulemüüri seadmes vigade diagnoosimisel tuleb kasutada süsteemset ning loogilist lähenemist. Kasutada *OSI* mudelit, kus vea diagnoosimist alustatakse esimesest tasemest (Füüsiline kiht) ja liigutakse järjest ülespoole. Sellega tagatakse vea analüüs nii riistvaraliselt kui tarkvaraliselt.
   6. Tulemüüri seadme väljavahetamisel peab olema võimalik taastada värskeim versioon tulemüüri konfiguratsioonist. Tulemüüriseadme konfiguratsiooni taastamise eest vastutab IT-teenusepakkuja võrguadministraator, kellel peavad olema vastavad teadmised, et varundatud konfiguratsioonifailist seadistust taastada.
   7. Enne tulemüüriseadme tarkvara uuendust, tuleb teha varukoopia olemasolevast konfiguratsioonist, et tagada tagasipöördumisvõimalus eelnevale tarkvaraversioonile (nt uuenduse käigus tõrke korral).
   8. Tulemüüri varundatud konfiguratsioonifail peab olema krüpteeritud või parooliga kaitstud keskkonnas. Konfiguratsioonifaili testimine toimub kas iga suurema konfiguratsioonimuudatuse korral, kuid mitte vähem kui kord kvartalis.
   9. Tulemüüriseadme rikke korral ei tohi tekkida olukord, kus KOV võrk ei ole piisavalt kaitstud.
3. **Riistvaralised nõuded ja rikke korral käitumine**
   1. Tulemüüri seadmetel peab olema hooldusleping KOV ja IT-teenusepakkuja vahel, mis määrab IT-teenusepakkuja vastutavaks tulemüüri rikete lahendamisel.
   2. IT-teenusepakkuja töötajatel peab olema vastav väljaõpe seadmete asendamiseks rikke korral.
   3. Tulemüüri tõrke korral tuleb informeerida IT-teenusepakkujat. Olukorras, kus tulemüüri seadmel on riistvaraline viga ning vajab väljavahetamist, peab IT-teenusepakkujal olema saadaval sama tüüpi/funktsionaalsusega varuseade või komponendid seadme parandamiseks. Asendatav tulemüüriseade ei tohi olla aladimensioneeritud.