**Algatamise eest vastutavad:** ametiasutuse/ettevõtte juhtkond, IT-turvaosakond  
**Rakendamise eest vastutavad:** IT-turvaosakond  
  
**ISKE Kataloog:** Versioon 8.06  
**ISKE Meede:**  M 2.279

Marsruuterite ja kommutaatorite turvapoliitika  
KOV võrkudes

Kohalike omavalitsuste võrkude seadistamisel on väga oluline roll kasutatavatel marsruuteritel ja kommutaatoritel. Seadmete konfigureerimisel tuleb lähtuda turvatehnilistest nõuetest.

1. **Ligipääs ja haldamine**
   1. Marsruuteritele ja kommutaatoritele (edaspidi võrgusüsteemid) peab olema tehtud eraldi administreerimisvõrgu kaudu ligipääs (VLAN). Samuti võib kasutada võrgusüsteemide konfigureerimiseks krüpteeritud ühendust. Kohapealset konsooli tuleb kasutada ainult hädaolukorras (nt kui administreerimisvõrk ja krüpteeritud ühendused on tõrkeolekus).

Auditeerijad peavad saama kasutada samu liideseid.

* 1. Võrgusüsteemidele tohib ligipääs olla ainult IT-teenusepakkuja võrguadministraatoril.  
     Võrguadministraatorite lisandumisel, kes ei ole IT-teenusepakkuja töötajad, tuleb ligipääsud KOV-ga eraldi kokku leppida.
  2. Võrgusüsteemide 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).
  3. Võrgusüsteemide ligipääsu seadistamisel tuleb ära keelata kõik krüpteerimata ning ebaturvalised protokollid.

1. **Turvalisus ja seadistamine**
   1. Võrgusüsteemide seadistamisel peab pooldama piiravat konfigureerimisstrateegiat. Ei tohi lubada põhjendamatuid protokolle ega kasutada ebaturvalisi ühendusi.
   2. Esmasel seadistamisel tuleb võrguseadmetel eemaldada *default\** konfiguratsioon. Samuti peab esmasel seadistamisel veenduma, et esimesena seadistatakse turvaline konfigureerimisliides (VLAN või krüpteeritud ühendus).
   3. Võrgusüsteemide tarkvara ning püsivara tuleb viia kõige värskemale ning turvalisemale versioonile. Samuti tuleb silmas pidada, et võrguseadmete kõige värskem tarkvara ning püsivara versioon ei pruugi olla alati kõige turvalisem. Võimalusel kasutada tootja poolt pikalt testitud ning kõige turvalisemaks märgitud tarkvara ning püsivara versiooni.
   4. Võrgusüsteemide seadistamisel peab olema võimalik kasutada erinevaid räsialgoritme (SHA256, SHA512) ning krüpteerimisalgortime (AES128,192,256).
   5. Võrgusüsteemide peal ei tohi olla paroolid lihtsas tekstis. Paroolid kui ka konfiguratsioonifail peab olema krüpteeritud kujul.
   6. VLAN-ide ja VPN-ide konfigureerimisel peab olema selgelt kommenteeritud, mille jaoks vastav seadistus tehtud on. VPN-ide konfigureerimisel peab kasutama IPSeci standardit koos sümmeetriliste kürpteerimisalgoritmidega ning võtmevahetus algoritmidega. Lisaks võib kasutada ka SSTP tüüpi VPN ühendusi.
   7. Olemasolevasse võrguhaldusesse võrgusüsteemide integreerimine peab olema võimalikult lihtne ning loogiliselt üles ehitatud. Nii seadmete soetamisel kui ka väljavahetamisel tuleb toetuda seadmete omavahelisele integreerumistasemele ning nõuete profiilist tulenevatele ettekirjutustele.
2. **Logid**
   1. Võrgusüsteemide konfigureerimisel peab olema võimalik logidest näha kõiki toimunud muudatusi. Samuti peab olema näha logidest ebaõnnestunud sisselogimiskatseid ning sellest peab jõudma ka automaatne teavitus IT-teenusepakkuja võrguadministraatorile.
   2. Logifailid peavad asuva seadme peal või krüpteeritud kujul välisel andmekandjal. Lisaks võib logisid hoida eraldi logiserveris.
   3. Logide analüüsimine peab toimuma iga kord, kui on konfiguratsioonis tehtud suurem muudatus, kuid mitte vähem kui kord ühe kuu jooksul.
3. **Andmevarundus**
   1. Võrgusüsteemide konfiguratsioonifaili peab regulaarselt varundama. Varundatud faili tuleb hoida krüpteeritult või parooliga kaitstud keskkonnas. Varundamine toimub kas iga suurema konfiguratsioonimuudatuse korral või kindlaks määratud perioodi tagant.
   2. Võrguseadmete hävimise korral peab olema võimalik varundatud konfiguratsioonifailist taastada võimalikult värske versioon.
4. **Rikked**
   1. Võrgusüsteemide rikete korral tuleb tagada seadmete turvaline ligipääs. Ei tohi tekkida ligipääsu võrgusüsteemidele väljaspool administratiivset võrku või kasutades mitte-krüpteerituid ühendusi.
   2. Riketele tuleb reageerida esimesel võimalusel või vastavalt turvatasemele.
   3. Olukorras, kus seadmele puudub läbi turvaliste administreerimisliideste ligipääs, tuleb kasutada koha peal oleva konsooli porti.
   4. Võrgusüsteemide teadaolevatest riketest tuleb esimesel võimalusel teavitada IT-teenusepakkujat. Samuti tuleb tagada võrgusüsteemidele füüsiline ligipääs volitamata isikutel (nt tõrke korral omavoliline seadme vooluvõrgust välja tõmbamine).
   5. Võimalikest turvaintsidentidest tuleb koheselt teavitada IT-teenusepakkujat.
5. **Dokumenteerimine**
   1. Võrgusüsteemides tehtud konfiguratsioonimuudatusi peab dokumenteerima IT-teenusepakkuja, kasutades selleks vastavaid tarkvaralisi lahendusi. Dokumentatsiooni järgi peab olema võimalik tuvastada toimunud sündmusi.
   2. Loodud dokumentatsioon peab olema lihtsasti arusaadav. Näiteks peab olema võimalik seda kasutada võimalike rikete tuvastamiseks, mis on tekkinud seadistamise käigus.

*Default* konfiguratsioon – seadme esimesel käivitamisel olemasolev konfiguratsioon. Tavaliselt sisaldab kõiki elemente, et alustada seadme edukat kasutamist. Tihtipeale kasutatakse rünnakuvektorina, kuna teada on konfiguratsiooni elemendid ning vahepeal ka vaikeparoolid.