Lisa 2. Tehniline kirjeldus

1. Sissejuhatus

Käesoleva hanke objektiks on järgmise põlvkonna tulemüür (Next-Generation Firewall, NGFW), millel on rakendustaseme (Layer 7) liikluse töötlemise võimekus. Seade peab lisaks tavapärasele võrguliikluse filtreerimisele suutma süvitsi analüüsida ja tuvastada rakendusepõhist liiklust, olenemata kasutatavast pordist või protokollist.

Seadmel peab olema:

- **IPS (Intrusion Prevention System)** funktsionaalsus – ründeid ennetav süsteem, mis suudab reaalajas tuvastada ja blokeerida pahatahtlikke tegevusi võrguliikluses.
- **IDS (Intrusion Detection System)** funktsionaalsus – ründeid tuvastav süsteem, mis jälgib liiklust ja annab teavitusi kahtlaste või lubamatute tegevuste kohta.

Kokkuvõtlikult peab hanke tulemusena soetatav lahendus tagama organisatsiooni võrgukeskkonna kaitse mitte ainult traditsioonilisel pordi- ja aadressipõhisel tasemel, vaid ka rakenduse- ja sisupõhisel tasemel, pakkudes terviklikku nähtavust, kaitset ja kontrolli.

2. Hanke eesmärk

Hanke eesmärk on soetada ja kasutusele võtta kaasaegne võrgu turbelahendus, mis tagab organisatsiooni sisevõrgu ja infosüsteemide kaitse väliste ja sisemiste rünnete eest. Tegemist on olemasoleva lahenduse uuendamisega seoses lahenduse elukaarega, kusjuures uus lahendus peab olema jätkusuutlik ja vastama ka tulevikus kasvavatele turvanõuetele.

Lahendus peab võimaldama:

- rakendustaseme (L7) liikluse detailset analüüsi ja kontrolli,
- pahatahtliku tegevuse tuvastamist ja ennetamist reaalajas,
- turvanõuetele vastavat funktsionaalsust (IPS ja IDS),
- logimise, auditeerimise ja seire võimekust, mis võimaldab turvajuhtumitele kiirelt reageerida.

Seadmete valik on suunatud Palo Alto ja Fortineti (**või „sellega samaväärne“ või parem**) lahendustele järgmiste asjaolude tõttu:

- keskhalduslahendused on organisatsioonis juba kasutusel, seega hanke eesmärgiks on olemasoleva lahenduse elukaare pikendamine ja uuendamine.
- administraatoritel on olemas kogemus ja kompetents nimetatud tootjate lahenduste haldamisel, mis tagab efektiivse ja kulutõhusa kasutuselevõtu ning käitamise.
- kuluefektiivsus – olemasoleva kompetentsi tõttu ei ole vajalik täiendav koolitus ega keerukas migratsioon, mis vähendab hankijale hanke kogukulu ja riske.

- lahenduste vähesus halduses – piirates kasutatavate turbelahenduste arvu, tagatakse organisatsiooni keskkonna lihtsam haldus, väiksemad kulud ja ühtlasem kompetents meeskonnas.

Uue lahenduse kasutuselevõtt aitab vähendada infoturberiske, tõsta võrgukeskkonna töökindlust ning täita regulatiivseid ja standardipõhiseid nõudeid, mis on seotud andmekaitse ja küberturvalisusega.

3. Tehnilised nõuded

Hanke käigus hangitakse järgmised komponendid:

- **2 seadet** paigaldamiseks kõrge töökindlusega (High Availability, HA) klastrisse,
- **1 seade** eraldiseisva lahendusena,
- **keskhaldustarkvara** kuni 10 seadme haldamiseks,
- **keskne logilahendus** hallatavate seadmete logide kogumiseks ja analüüsiks(võib sisalduda keskhaldustarkvara funktsionaalsuses või olla eraldi komponent),
- **litsentsid ja tugiteenus** kõikidele komponentidele perioodiks vähemalt 60 kuud. https://www.paloaltonetworks.com/services/support/customer-support-plan või https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-services.pdf

4. Riistvara – 3tk

1) **Palo Alto PA-3430 (või „sellega samaväärne“ või parem)**

või

2) **Fortinet FortiGate 901G(või „sellega samaväärne“ või parem)**

5. Keskhaldus- ja logihaldustarkvara

Lahendus peab võimaldama seadmete **keskset logihaldust**, mis katab kogu hankega soetatava infrastruktuuri.

- Lahendus peab suutma töödelda ja talletada logisid mahus kuni **15 GB päevas**.
- Vajalikud komponendid (sh võimalikud eraldi seadmed, litsentsid ja tugi) peavad olema pakkumuses kaasas.
- Keskhaldus- ja logihaldustarkvara lahendused peavad olema **virtuaalserveri põhised** ning peavad olema saadaval **Nutanix keskkonnale**.

- Keskhaldus- ja logihaldustarkvara funktsionaalsust tagavad litsentsid peavad olema **eluaegse kehtivusega** (perpetual).

6. Litsentsid ja tugiteenus

Lahendusega peab lisaks olema kaetud järgmine funktsionaalsus (vastavuses pakkumuse maksumuse vormiga):

- **Laiendatud URL-põhine filtreerimine**,
- **Ründe- ja pahavaratõrje** (sh IPS/IDS, pahavara- ja DNS turve),
- Turvepoliitikate tegemise võimalus vastavalt LDAP kasutajagruppidele. Sealhulgas tulemüüride võimekus tuvastada kasutaja identiteet (User-ID funktsionaalsus) Windows Active Directory kontrolleri logide ja/või syslogi põhjal. Kõik User-ID funktsionaalsusega kaasnevad komponendid peavad olema lahenduses kaasas **ilma lisakuludeta,**
- **Tootjapoolne ametlik premium taseme tugi** (sh tarkvarauuendused ja turvapaigad) kõigile komponentidele.

Kõik eeltoodud litsentsid ja tugiteenused peavad olema kehtivad vähemalt **5 aastat**. Pärast litsentside ja tugiperioodi lõppemist peab lahenduse **baasfunktsionaalsus säilima:**

- **tulemüüri- ja NAT-funktsioonid,**
- **olemasolevad turvapoliitikad ja reeglid,**
- **VPN-funktsionaalsus,**
- **routing ja haldusliides.**

Tellimuspõhised teenused (sh IPS/AV signatuuride uuendused, URL kategooriate ja DNS turbeandmebaaside uuendused, reaalajas pilveteenused, tootjapoolne tehniline tugi ja tarkvarauuendused) võivad pärast litsentsi lõppemist katkeda. Selliste teenuste lõppemine ei tohi piirata seadme töövõimet ega katkestada baasfunktsionaalsuse kasutamist.

7. Andmete töötluse nõuded

- Lahendus peab tagama, et tulemüüri läbivat võrguliiklust ei saadeta tootja pilveteenusesse töötlemiseks ega analüüsimiseks. Sellise funktsionaalsuse olemasolul peab olema võimalik seda deaktiveerida.
- Lubatud on tootjapoolsete tarkvara- ja turvauuenduste allalaadimine pilvest, kuid mitte liiklusandmete edastamine väljapoole organisatsiooni infrastruktuuri.

- Kõik liikluse analüüsi- ja turbefunktsioonid peavad toimuma lokaalselt organisatsiooni hallatavates seadmetes või virtuaalsetes komponentides.

8. Lisanõuded pakkumisele:

- Seadmete transpordi kulud hankija esitatud aadressile kannab pakkuja ja see peab sisalduma pakkumuse hinnas.
- Tarne: Mäealuse 2/2, Tallinn
- Kontakt: Ardi Ahi - 5197 1440; ardi.ahi@smit.ee
- Kõigi hangitavate seadmete loetelu osas kehtib RHS § 88 lg-s 6 sätestatud samaväärsuse klausel.
- Pakkuja võib pakkuda ka hankija poolt nõutud seadmetega samaväärseid seadmeid, kuid sellisel juhul peab pakkuja hankijale esitama pakkumuse koosseisus ka lisadokumendid ja selgitused, tõendamaks pakutava samaväärsust hangitavate seadmetega ning ühilduvust hankija olemasolevate seadmetega. Samaväärsed tooted ei tohi tekitada mistahes häireid või takistusi hankija olemasolevate seadmete töös.
- Samaväärsete toodete pakkumisel on pakkuja hankija nõudmisel kohustatud oma kulul tarnima ja tööle seadistama hankija poolseks testimiseks (ühe nädala jooksul) pakutava toote näidisseadme(-ed) enne hankija poolse otsuse tegemist, et hankijal oleks võimalik veenduda pakutavate seadmete samaväärsuses ja hankija olemasolevate seadmetega ühilduvuses.
- Kui näidisseadmete testimise või pakkuja poolt esitatud tõendite alusel ei ole hankijal võimalik üheselt veenduda seadmete sobivuses hankija arvutivõrku ja nende ühilduvuses olemasolevate seadmetega, ei kohustu hankija selliseid seadmeid ostma.
- Samaväärsete seadmete ja samaväärsust tagavate seadmete (sh litsentside) hind peab sisalduma pakkumuses.
- Näidisseadmete testimisega seonduvad kulud kannab pakkuja.
- Seadmed peavad olema uued ja originaalpakendis.
- Esitatud tootjapoolne esindusõigus.
- Seadmete juurde kuuluv tarkvara (nt operatsioonisüsteem) peab olema ettenähtud kasutamiseks hankija asukoha regioonis.
- Garantii peab olema no drive returniga kõikidel kastidel.