Lisa 4 - Visioon/ettepanek interaktiivse infoturbe halduse tööriista tellimiseks

Vajaduse hinnang

Käesoleval hetkel puudub turul Eesti avaliku – ja erasektori ettevõtetele mõeldud, peamisi infoturbe halduse protsesse sisaldav elektrooniline tööriist. Antud tööriistast tunnevad eriti puudust elutähtsate teenuste osutajad (ETO-d), kelle infoturve ei ole nii reguleeritud kui avaliku ja riigisektori ettevõtete puhul, mille andmekogude infoturbe rakendamiseks on kohustuslik rakendada ISKE meetmeid. Samas on ETOd kohustatud koostama infoturbealaseid riskianalüüse ja infoturbe tegevustest ning toimunud infoturbe intsidentidest tsentraalselt raporteerima. Kuna kõik ETOd tagavad ja haldavad infoturvet iseseisvalt, vastavalt oma võimekusele ja olemasolevatele ressurssidele, on infoturbe tase hetkel ettevõtetes väga kõikuv.

Puudub keskne ülevaade ETOde infoturbe olukorrast ja võimekusest tagada elutähtsa teenuse pakkumine pärast infoturbe intsidendi toimumist. Olukorda võiks leevendada sarnase infoturbehalduse tööriista juurutamine erinevates ettevõtetes, mis aitab luua kõigile ühtsed alused infoturbe halduse süsteemi loomiseks ja standardiseeritud aruandluse infoturbe halduse piisavuse hindamiseks.

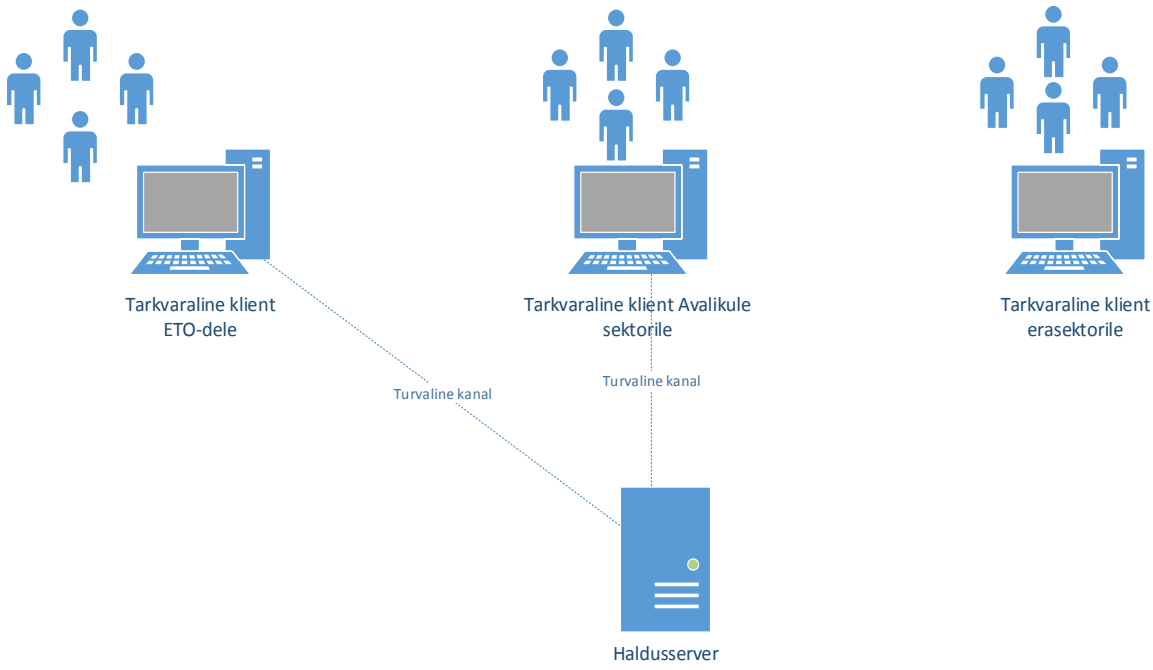
Kontseptsioon

Ühise infoturbe halduse tööriista rakendamine kergendaks ettevõtetes infoturbehalduse protsesse, tagaks turvalise keskkonna suhtluseks erinevate ettevõtete infoturbejuhtide vahel ning aruannete ning intsidendiraportite esitamiseks regulaatoritele. Infoturbe halduse tööriist lihtsustaks infoturbejuhi tööd, koondades kogu vajaliku operatiivse informatsiooni tööriista töölauale, mistõttu puudub vajadus jälgida samaaegselt erinevate programmide teateid ja töölaudu. Lisatud kalendrivaade aitab meeles pidada, tehtuks märkida ning hiljem leida ja analüüsida rutiinseid ja perioodilisi tegevusi. Tööriista on integreeritud infoturbe riskide register, kus toodud riskid on seostatud üksikute infoturbemeetmetega. Turvaline juurdepääs tööriistale tagatakse läbi rollipõhise juurdepääsuõiguste süsteemi rakendamise. Juurdepääsu võivad omada kõik asjasse puutuvad töötajad, vastavalt teadmisvajadusele. Aruandlus annab igal ajahetkel hinnata infoturbe meetmete vastavust valitud standardile. Samuti võib ettevõtte juht saada kiirülevaate käsilolevatest infoturbe projektidest või näha, mitu kriitilise tähtsusega infoturbe intsidenti on hetkel avatud.

Kontseptuaalselt näeme ette tööriista kasutamist kolmes erinevas režiimis (vt Joonis 1. Infoturbehalduse tööriista nägemus)

1. **Infoturbe halduse tööriist iseseisvas klientrežiimis**, mille puhul puudub ühendus keskse haldusserveriga. Kogu rakendus ja andmestik paikneb lokaalses tööjaamas või lokaalses serveris (joonisel Tarkvaraline klient erasektorile) .
2. **Infoturbe halduse tööriist avalikule sektorile**, mille puhul tööriist on eelkonfigureeritud ISKE meetmetega. Ettevõttes paiknev tööriist on ühendatud turvalise kanali kaudu keskse haldusserveriga. Muudatuste puhul ISKE meetmete kataloogis uuendatakse automaatselt ka tööriistas asuvaid meetmete katalooge. Lisandub audiitori roll, kes saab infoturbe halduse tööriista kasutades anda oma hinnangu meetme rakendamisele ning hiljem jälgida, kas tema poolt antud soovitused on ettevõttes rakendatud.

3. **Infoturbe halduse tööriist ETOdele,** mille puhul on võimalik kasutada keskset haldusserverit regulaatoritega ja teiste infoturbe juhtidega suhtlemiseks ning regulaatorile aruannete saatmiseks. Ettevõte saab valida, millist infoturbe meetmete kataloogi (ISKE, NIST, ISO 27001 või spetsiaalselt ETOde jaoks loodud infoturvameetmed) ta kasutab. Võimalik on ise luua täiendavaid infoturvameetmeid.



Joonis 1. Infoturbehalduse tööriista nägemus

Tööriista funktsionaalsuse kirjeldus

Infoturbe halduse tööriist sisaldab endas erinevaid mooduleid. Nendeks mooduliteks on:

- **Infoturbe meetmete moodul**
  - Sisaldab erinevatel infoturbe standarditel põhinevaid eeldefineeritud (NIST, ISO27001, ISKE jt) või ise koostatud infoturvameetmeid. Kasutajal on võimalik valida millist infoturbe standardit või milliseid turvameetmeid ta soovib rakendada. Samuti on kasutajal võimalik kombineerida turvameetmete valim erinevate standardite põhjal. Iga meetme põhiandmestikku moodustab meetme kategooria, alamkategooria, meetme kirjeldus ja vajalik küpsustase (1-5).
  - Iga meetme kohta on võimalik sisestada rakendatuse staatus, vastutaja, rakenduse tegevusplaan ning ülevaatamise tähtaeg.
  - Moodulis on võimalik sisestada ja täiendada seisu meetmete rakendamise staatuse kohta Staatused on järgmised:
    Rakendatud – rakendatus 86- 100%
    Osaliselt rakendatud – rakendatus 51 – 85%
    Rakendamisel – rakendatus 16- 49%
    Rakendamata – rakendatus 0 – 15 %
  - Moodulis on võimalik valida ettevõtte soovitav infoturbe küpsustase, mille alusel kuvatakse rakendamisele kuuluvaid meetmed. Küpsustaseme määratlemiseks võib

kasutada erinevaid süsteeme (nt. ISKE puhul 1-L, 2-M, 3-H) Soovitavat küpsustaset kasutatakse ka meetmete rakendamise aruandluse juures.
    - Infoturbe juhi tööplaani täiendamiseks saab määrata ajas korduvaid tegevused (nt. kvartaalne kasutusõiguste inventuur). Korduvuse (nädal, kuu, kvartal, poolaasta, aasta) saab märkida eraldi iga vastava meetme juures.
    - Moodulis asub omaette tabelina eeldefineeritud ohtude kataloogid. Ohtude kataloogi on võimalik kasutada riskianalüüsi läbiviimiseks. Kasutades ohtude kataloogi, saab infoturbe halduse tööriistas koostada riskiregistri. Iga riski juures saab näidata riski tõenäosust (skaalal 0-5) ja mõju (skaalal 0-5)
    - Riskiregistris defineeritud riske on võimalik seostada üksikute infoturvameetmetega. Juhul kui muutub meetme rakendamise staatus, pakutakse võimalust vähendada/suurendada antud meetmega seotud riskide tõenäosuse või mõjuhinnanguid. Seega tööriista sisestatud esmase riskianalüüsi tulemusi saaks jooksvalt uuendada, vastavalt seotud turvameetmete rakendamise staatusele.
    - Moodulist on võimalik eksportida erinevaid raporteid meetme rakendamise staatuse kohta (nt vastutajakohaseid raporteid, ajaplaane, kõige prioriteetsemate meetmete rakendamise staatuseid jne).

- **Teavituste ja intsidentidest teavitamise moodul**
    - Moodul võimaldab sisestada infoturbe intsidente, täites selleks kõik vajalikud väljad käsitsi
    - Sisestatud infotube intsidendile on võimalik määrata vastutav isikut. Vastutav isik saab kohe vastava teate läbi valitud suhtluskanali (e-post, SMS, Slack vms) ja saab asuda intsidenti lahendama
    - Intsident on avatud niikaua, kuni ta märgitakse suletuks. Informatsiooni kasutatakse tööriista poolt genereeritavas infoturbe aruandes.
    - Mooduli kaudu on võimalik CERT-EE-le, elutähtsaid teenuseid korraldavale asutusele või Andmekaitse Inspektsioonile edastada teavitusi/raporteid infoturbe intsidentidest. Teavitusi saadetakse üle turvalise sidekanali, välistades niimoodi võimaliku tundlikute andmete lekke, kui raporteid saadetakse turvamata e-posti või muid sidekanaleid kasutades.
    - Intsidentide teavitamiseks ja muude infoturbe aruannete edastamiseks kasutatakse tööriista sisse ehitatud standardseid vorme.
    - Samuti on võimalik suhelda (üle turvalise kanali) teiste asutustega ning saada teavitusi CERT-EE-lt või RIA-lt võimalikest infoturbe ohtudest.

- **Monitooringu- ja analüüsi moodul**
    - moodulisse on võimalik importida erinevatest välistest süsteemidest (analüüsivahendid, logide generaatorid, konfiguratsioonihaldusvahendid jne) infoturbe staatust kuvavaid andmeid.
    - Import välistest süsteemidest toimub läbi eeldefineeritud APIde. Äriloogika (filtrid, KPIde arvutused) tehakse ära välises süsteemis endas või vahekihis, enne infoturbe halduse tööriista eksportimist.
    - Antud tööriist jätab kasutajate valida, milliste väliste SIEM süsteemide, võrgumonitooringu vahendite või turvanõrkuste analüsaatoritega liidestus luuakse ja millistele tingimustele vastavaid andmeid erinevatest monitooringutarkvaradest või seadmetest (tulemüüri logid, võrguliikluse monitooringu logid jt) kuvatakse.

Eeldefineeritud API kasutamine tagab infoturbe halduse tööriista sõltumatuse kasutatavatest andmeallikatest.
    - Enam kasutatavate monitooringutarkvarade (nt Nagios või muud RIA poolt soovitatud tarkvarad) jaoks võiks tööriistas olla eelkonfigureeritutud liidestused.
    - Tööriist ei ole mõeldud asendama spetsiaalseid analüüsitarkvarasid. Peamine funktsionaalsus on eelnevalt töödeldud ning prioritiseeritud, erinevatest allikatest pärit informatsiooni kuvamine kõrvuti, ühtsel töölaual.
    - Moodul on suuteline erinevatest sisendallikatest saadud info põhjal koostama visuaalselt sarnases stiilis graafikuid ning diagramme.
    - Moodulit on võimalik seadistada saatma teavitusi ründekatsetest või anomaaliatest sms-i, e-posti jt sidekanalite teel infoturbejuhile või teistele määratud isikutele. See funktsionaalsus võimaldab töötajatele saadetavaid teavitusi tsentraalselt hallata, ilma et peaks seda tegema igas analüüsitarkvaras eraldi.

- **Infoturbejuhi töölaud**
    - Tulenevalt rakendamata või rakendamisel olevate meetme juures määratud kuupäevadest ja korduvaid tegevusi nõudvate meetmete juures märgitud tsüklilisusest koostatakse ja kuvatakse infoturbe juhi (või mõne muu sisse loginud tööriista kasutaja) personaalne tööplaan/kalender. Kalendris kuvatavaid tööülesandeid saab kas märkida käsil olevaks, tehtuks või määrata neile uus tähtaeg.
    - Töölaual kuvatakse monitooringu- ja analüüsimoodulist tulevaid teavitusi, vastavalt eeldefineeritud prioriteetsustasemele ja muudele rakendatud filtritele.
    - Kuvatakse haldusserveris paikneva sõnumivahetuskeskkonna viimased teated
    - Kuvatakse monitooringu- ja analüüsimoodulis defineeritud infoturbe näidikud (nt. lahendust ootavate infoturbe intsidentide arv)

Haldusserveri funktsionaalsuse kirjeldus

Haldusserver suhtleb infoturbe tööriista tarkvaraliste klientidega. Haldusserveris asub keskne infoturbe intsidentide raportite andmebaas. Kuna kasutatakse ühtsetel alustel toimuvat intsidentide kategoriseerimist, on lihtne saada igal ajahetkel saada ülevaadet infoturbe intsidentide statistikast üle kõigi haldusserveriga ühendatud ettevõtete.

Haldusserveris asub klientide haldusmoodul, mille kaudu saab lisada või eemaldada kliente (süsteemi kasutavaid ettevõtteid). Samuti saab läbi antud mooduli anda ja piirata klientide õigusi haldusserveris asuva informatsiooni nägemiseks.

Läbi haldusserveris asuva teavituste saatmise mooduli on võimalik teavitada kas kõiki kliente korraga või valitud kliente erinevatest intsidentidest või ohtudest või jagada muud olulist informatsiooni. Lisaks on võimalik üle turvalise sidekanali ettevõtte infoturbejuhtidega suhelda ning turvaliselt informatsiooni vahetada.

Haldusserveris asub keskne intsidentide raportite põhine analüüsi moodul. Antud moodul analüüsib saadetud intsidente ja koostab analüüsi põhjal aruandlust enam esinevatest intsidenditüüpidest ja riskidest. Kliendid, kellel on haldusserverile vastav juurdepääs, saavad vaadata keskset intsidentide statistikat ja aktuaalsete riskide graafikuid ning seda informatsiooni kasutada oma ettevõtte riskide analüüsil ja hindamisel.

Peamised tehnilised ja mittefunktsionaalsed nõuded

Loodavale infoturbe halduse tööriistale kohalduvad järgnevad nõuded:

- Tööriist peab töötama/funktsioneerima eraldiseisvana lokaalses arvutis või ühendatuna keskse haldusserveriga
- Peab olema võimalik kasutada eeldefineeritud ja koostada ise uusi väljavõtteid/raporteid rakendatud ja rakendamata turvameetmetest;
- Peab olema võimalik defineerida ja kasutada vorme info edastamiseks CERT-EE-le ja regulaatoritele;
- Peab olema võimalik saata/vastu võtta teavitusi CERT-EE-lt ja regulaatoritelt;
- Peab olema võimalik saata teateid, tekitada teemakohaseid suhtluskeskkondi ning vahetada turvaliselt andmeid teiste, süsteemiga ühinenud ettevõtetega;
- Suhtlus haldusserveriga kui ka teiste asutustega peab toimuma üle turvalise kanali (VPN tunnel, x-tee jne);
- Tööriist omab turvalist, mitmefaktorilist autentimissüsteemi (nt ID-kaart)
- Tööriist omab paidlikku õiguste haldamise süsteemi vastavalt kasutaja rollile (Infoturbejuht, IT administraator, riskijuht jne). Rollipõhisele õiguste andmise mudelile lisaks saab anda igale kasutajale individuaalseid õigusi.
- Kõik tööriista sisse- ja väljalogimised ning tehtud andmesisestused logitakse