RIIGI INFOSÜSTEEMI AMET

Juhis ettevõtte küberturvalisuse baastaseme hindamiseks ja Küberpöörde teekaardi koostamiseks

Kaasrahastanud Euroopa Liit

ECCC

Versioon	***Avaldatud***	***Muutus***
0.5	*14.02.2023*	*Töövariant*
1.0	*03.03.2023*	*- teekaardi koostamise soovituslik käik* *- kommentaarid skoobi ja tegevuskava osas*

Käesolev dokument sisaldab metoodikat, mis on mõeldud Küberpöörde toetusmeetme tarbeks valmiva teekaardi koostamiseks. Dokument on kättesaadav RIA koduleheküljе kaudu küberpöörde metoodika nime all aadressil:

https://www.ria.ee/kuberturvalisus/riiklik-koordinatsioonikeskus-ncc-ee/riiklik-koordinatsioonikeskus-ncc-ee

Lisainfo teekaardi metoodika ja koostamise kohta: Lauri Tankler, lauri.tankler@ria.ee

Küberpöörde teekaart on ettevõtte küberturvalisuse hetkeolukorra kaardistus, milles antakse hinnang ettevõtte küberturvalisuse hetkeseisule, tuuakse välja puudujäägid ning küberturvalisuse taseme tõstmiseks vajalikud tegevused ja ettepanekud. Teekaardi põhieesmärk on hinnata ettevõtte infosüsteemide infoturbealast olukorda, võttes aluseks rakendatud tehnilised-, füüsilised ja organisatoorsed turvameetmed ning vigade ilmnemise korral teha ettepanekuid parandusteks.

Teekaardi alaeesmärk on tõsta ettevõtja juhtkondade teadlikkust ning tuvastada, kas ja kuidas on potentsiaalsel ründajal võimalik saavutada ligipääs ettevõtja kriitilistele infosüsteemidele, seadmetele, arvutivõrkudele ja andmetele eesmärgiga oluliselt häirida ja/või katkestada kriitilise äriteenuse toimimist.

Teekaart on aluseks RIA ja EASi loodud küberpöörde toetuse andmiseks ning toetuse andmiseks kasutamisel peab see sisaldama toetuse andmise tingimuste punktis 5.4 nimetatud osiseid:
1) ajakohane organisatsiooni **küberturvalisuse taseme kaardistus**, sh võrkude, tulemüürireeglite, kaugligipääsude, serverite võrkude ja haldusvõrkude, valvesüsteemide võrkude, automaatikavõrkude, serveri ja seadmeruumide füüsilise turbe võrkude, riskianalüüside ülevaatust, **hinnang** ettevõtja töötajate teadlikkusele küberturvalisuse riskidest ja **ettepanekud** küberturvalisuse taseme tõstmiseks;
2) hinnangut leitud **turvanõrkuste lahendamise prioriteetsusele ja arenduse keerukusele**. Hinnang on **piisava täpsusastmega** sisendiks edasiste arendustegevuste elluviimiseks koostatava dokumentatsiooni ja tegevuse hinnastamiseks.
3) Hinnangut punktis 2 nimetatud arendustegevuste läbiviimise **kestusele, järjestatust ja ühe (1) aasta tegevuskava**.

Küberpöörde teekaardi toetuse taotlemise protsess on detailselt kirjeldatud EASi koduleheküljel aadressil https://eas.ee/grants/kybertoetus/. Käesolev metoodika on mõeldud juhendmaterjaliks küberturvalisuse hindamist tegevale teenusepakkujale.

I Teekaardi koostamise soovituslik käik:

1. kokkuleppe sõlmimine ettevõtja ja teekaardi koostaja vahel;
2. ettevõtja küberküpsustaseme hindamine ja skoobi ettevalmistamine (suhtlus kliendiga, vajadusel küsitlusleht vms)

   Iga ettevõtte kaardistus ja skoop on erinev. Käesoleva metoodika puhul soovitame lähtuda riskipõhiselt – vastavalt ettevõtte tegevusalale, tehnoloogiatele, küpsusele jne – ja põhjendada kliendile, miks etteantud aja jooksul on kõige mõttekam pöörata tähelepanu just nendele füüsilistele asukohtadele, võrkudele, tegevustele jne.

3. Protsesside kaardistamine, IT-keskkonnaga tutvumine (nt IT-dokumentatsiooni läbivaatus jms) ja tehnilised testid, mis ei vaja kohapeal käiku (välisperimeeter, veebilehed jne);
4. kohapealne ülevaatus, sh vajalikud tehnilised testid;
5. raporti kirjutamine;
6. raporti esitlemine ettevõtja juhtkonnale;

II Teekaardiks vajaliku kaardistuse skoop:

1. avalikust internetist potentsiaalsete rünnete sooritamiseks kasuliku informatsiooni kogumine ja tehniliste nõrkuste leidmine;
2. välisperimeeter ja avalikud veebilehed;

3. tulemüüri kasutus ja tulemüürireeglite ülevaatus;
4. kaugligipääsud – VPN, IPSEC tunnelid jm;
5. kontorite võrgud (x asukohta): tööjaamad ja serverid. Kontorite Wifi võrgud ja nende seadmed;
6. serverite võrgud ja haldusvõrgud;
7. vajadusel valvesüsteemid ja nende võrgud – läbipääsusüsteemid, videovalve;
8. vajadusel automaatikavõrgud – UPS-id, hooneautomaatika (x asukohta);
9. serveri- ja seadmeruumide füüsilise turbe vaatlus;
10. riskianalüüsi ja taasteplaanide olemasolu ja ülevaatus.

Teekaardi koostaja võib vastavalt oma äranägemisele skoopi vähendada (näiteks juhul, kui ettevõte ei kasuta kaugligipääse või tal puuduvad serverivõrgud vms). Sel juhul tuleb põhjendada teekaardi lõpparuandes, miks skoopi vähendati. Kui klient soovib taotleda teekaardi tegemiseks küberpöörde toetust, peab teekaart järgima miinimumnõudeid, mis on välja toodud toetuse andmise tingimuste dokumendis.

III Küberturvalisuse baastaseme hindamise ja teekaardi koostamise tegevused

1. Avalikust internetist potentsiaalsete rünnete sooritamiseks informatsiooni kogumine ja tehniliste nõrkuste leidmine.

Teekaardi koostaja ülesandeks on selgitada välja, mil määral on võimalik potentsiaalseteks rünneteks kasulikku infot ja tehnilisi nõrkusi leida avalikest allikatest. Muuhulgas peab koostaja skaneerima ettevõtja avalikku arvutivõrku, et leida potentsiaalseid nõrkusi.

Kasulikuks infoks loetakse nt tehnilist dokumentatsiooni, tootjate pakkumisi ja kasutatud referentse, töötajate nimesid koos töö- ja erialaste andmetega, seadmete tootjate ja mudelite täpseid nimetusi, konfiguratsiooni, kasutusjuhendeid, paikamata serverite või teenuste loetelu jms.

2. ja 3. Välisperimeeter ja tulemüürid

Teekaardi koostaja ülesandeks hinnata perimeetril olevate seadmete (võrguseadmed, tulemüürid, serverid jne) turvalisust puudutavate seadistuste vastavust üldlevinud headele tavadele ja ettevõtja infoturbepoliitikale sh. tulemüürireeglite ülevaatus.

Teekaardi koostaja ülesandeks on samuti kontrollida, kuidas on võimalik saavutada kontorivõrgust autoriseerimata ligipääs tundlikes ja halduskriitilistes võrkudes asuvate süsteemideni.

*Kodulehe puhul on pakkuja ülesanne kontrollida, kas kodulehe tarkvara ja pistikprogrammid (*plugins*) on tootja poolt toetatud, uuendatud viimasele versioonile ja ei sisalda teadaolevaid nõrkusi. Samuti kontrollib pakkuja, et kodulehe seadistused on turvalised ja administreerimise õigusega kontosid on mõistlikul hulgal ning nende kasutajad on tuvastatavad.*

4. Kaugligipääsud

Teekaardi koostaja ülesandeks on kontrollida, kas nii töötajate, koostööpartnerite kui ka haruüksuste kaugligipääsud kontori- ja kriitiliste äriteenuste osutamiseks vajalikele infosüsteemidele vastavad üldlevinud headele tavadele. Samuti peab pakkuja võimaluse korral tuvastama dokumenteerimata kaugligipääsud.

5. - 8. Võrgus olevate seadmete ja teenuste turvalisuse hindamine.

Teekaardi koostaja ülesandeks on hinnata erinevates võrkudes asuvate tööjaamade, serverite ja võrku ühendatud seadmete turvalisust puudutavate seadistuste vastavust üldlevinud headele tavadele ja ettevõtja infoturbepoliitikale (näiteks viirusetõrje olemasolu ja signatuuride uuendamine, operatsioonisüsteemi turvapaikade paigaldamine, keelatud tarkvara olemasolu, ebavajalike võrguteenuste olemasolu, administraatori konto ebaturvaline kasutamine, aegunud (rakendus)tarkvara kasutamine, võrguseadmete jt seadmete püsivara uuendamine jne).

Põhiline tähelepanu pöörata administraatorite ja võtmeisikute tööjaamadele ning serveritele, mille kaudu on võimalik pääseda ligi serveritele ning ärikriitilistele infosüsteemidele.
Wi-Fi võrkude puhul on teekaardi koostaja ülesanne kontrollida, kas nendest võrkudest on võimalik saavutada ligipääs ärikriitilistes võrkudes asuvate süsteemideni. Lisaks hinnata, kas potentsiaalsel ründajal on võimalik ära kasutada avalikes ruumides asuvaid WiFi tugijaamade kaabliühendusi.

9. Füüsilise turvalisuse hindamine

Teekaardi koostaja ülesandeks on hinnata, kas IT süsteemide, seadmete, oluliste seadmekappide, serveriruumide jne kaitseks on rakendatud piisavaid füüsilisi turvameetmeid, mis välistaks autoriseerimata isikute ligipääsu nendele (sh ka ettevõtja enda töötajate).

10. Riskianalüüsi ja taasteplaanide olemasolu ja testimine

Teekaardi koostaja ülesandeks on kontrollida, kas ärikriitiliste infosüsteemide jaoks on loodud asjakohased taasteplaanid ning anda hinnang, kas taasteplaanid on piisavalt põhjalikud, et nende abil oleks vajadusel võimalik reaalselt süsteeme taastada.

IV Tulem

Projekti lõpuks esitab teekaardi koostaja tellijale “Küberpöörde teekaardi” kirjaliku dokumendi ehk raporti, kus on kaardistatud ettevõtja küberturvalisuse hetkeolukord ja küberturvalisuse taseme tõstmiseks vajalike tegevuste ehk ettepanekute osa.

V Teekaardi ülesehitus

Küberpöörde teekaardi dokument peab minimaalselt sisaldama järgmisi punkte. Näidisraport on kättesaadav RIA koduleheküljel küberpöörde alamlehel. Teekaardi koostaja võib kasutada RIA poolt pakutavat teekaardi vormi või enda väljatöötatud vormi.

Üldosa

1. Sissejuhatus ja lühikokkuvõte
2. Teostatud tööde metoodika ja skoop
3. Leidude kokkuvõte ja peamised tuvastatud probleemid
4. Hinnang ressurssidele (oskusteave, aeg, finantsid jne) mille olemasolul on potentsiaalsel ründajal võimalik korraldada edukas küberrünnak ettevõtja süsteemide vastu, mille tulemusena katkeb ärikriitiline teenus ja/või on selle osutamine olulisel määral häiritud.
5. Järeldused ning ettepanekud

Tehniline osa

6. Testimise läbiviimiseks kasutatud tark- ja riistvara nimetused koos kirjeldustega, kasutatud metoodikate, standardite ja parimate praktikate kirjeldused
7. Ettevõtja IT-keskkonna üldine kirjeldus
8. Tähtsamad leiud (iga ilmnenud probleemi kohta peab aruanne sisaldama vähemalt järgmist):
    a. viide komponendile või süsteemile
    b. probleemi kirjeldus
    c. juhend probleemi esilekutsumiseks
    d. hinnang probleemi tõsidusele
    e. soovitused ja ettepanekud probleemi kõrvaldamiseks
    f. CVSS skoor (jätta välja, kui pole võimalik)

    (Kui probleem ilmneb korduvalt, nt turvanõrkus mitmes süsteemis, on mõttekas probleemi kirjeldada ühel korral ja tuua välja ilmnemise kord)
9. Ilmnenud probleemide koondtabel, kus pakkuja toob välja soovitusliku järjekorra probleemide lahendamiseks ja annab hinnangu probleemide lahendamise prioriteetsusele ja keerukusele (võttes aluseks nt probleemi tõsiduse ja lahendamiseks kuluva aja vms);
10. Hinnang ja lühike tegevuskava, milliste tegevustega saab ettevõte 1 aasta jooksul kõige paremini punktis 9 nimetatud soovitusi ellu viia.

    Lühike tegevuskava võiks sisaldada ettevõttele vajalikku tehtavate tööde nimekirja, millele oleks tal võimalik võtta hinnapakkumine. Näiteks soovitus vahetada nõrka vaikeparooli pole eraldi mõttekas lisada aastase tegevuskava hulka, sest see tuleks ära teha kohe, ilma hinnapakkumist võtmata. Lühikese tegevuskava põhieesmärk on pakkuda ettevõttele head sisendit, milliseid arendustöid oleks tal vaja kas ise teha või tellida, millele saab ettevõte taotleda ka Küberpöörde 2. taseme toetust.

Orienteeruv ajakulu, muud nõuded, selgitused ja täpsustused

- Orienteeruv ajakulu sõltub ettevõtte suurusest, arvutitöökohtadest, asukohtadest jne. Näiteks kahe füüsilise asukoha ja paarikümne arvutitöökohaga ettevõttes võiks RIA hinnangul kuluda intervjuude ja testimise läbiviimiseks kaheliikmelisel meeskonnal kohapeal ca 5 tööpäeva, millele lisandub aruannete koostamise ja testide ettevalmistamise aeg.
- Testide läbiviimiseks peab ettevõte võimaldama teenusepakkuja töötajatele ligipääsu oma arvutivõrgule. Tagada tuleb töökoha olemasolu (laud, tool ja juhtmega

võrguühenduse võimalus), samuti on oluline, et ettevõtte IT töötaja oleks valmis jooksvalt toetama hindamise läbi viimist. Täpsemad nõuded on mõistlik kokku leppida teenusepakkuja esindajaga.
- Testimine viiakse läbi toodangu keskkonnas, mis tähendab, et pakkuja peab kõik testid põhjalikult ette valmistama, kooskõlastama tellijapoolsete ekspertidega ning viima läbi suure ettevaatlikkusega.

Vaata lisaks ka näidisteekaarti RIA kodulehel.

Teekaardi lisaküsimused palume esitada:

Lauri Tankler
Teaduse ja arenduse koordineerimisosakond
Küberturvalisuse teenistus
Riigi Infosüsteemi Amet
Lauri.Tankler@ria.ee

Küsimused taotlemise, taotlemiseks vajamineva dokumentatsiooni ning nõustamise osas:

Anari Lilleoja
Tootejuht
Toetuste osakond
Ettevõtluse ja Innovatsiooni Sihtasutus
Anari.Lilleoja@eas.ee