Teekaardi hindamise vorm

1. Üldised nõuded teekaardile

	Osa	Jah	Ei	Kommentaar (vajadusel)
1	Organisatsiooni küberturvalisuse taseme kaardistus on ajakohane			
2	Teekaardis on ettepanekud küberturvalisuse taseme tõstmiseks			
2a	*Kui eelnev on jah* Ettepanekud küberturvalisuse taseme tõstmiseks on ajakohased ja piisavad			
3	Teekaardis on hinnangud leitud turvanõrkuste lahendamise prioriteetsusele ja arenduse keerukusele			
3a	*Kui eelnev on jah* Hinnangud on ajakohased ja piisava täpsusastmega sisendiks edasiste arendustegevuste elluviimiseks koostatava dokumentatsiooni ja tegevuse hinnastamiseks			
4	Teekaardis on hinnang, kui palju võtavad aega turvanõrkuste lahendamiseks välja toodud vajalikud arendustegevused			
5	Teekaardis on olemas turvanõrkuste lahendamiseks vajalike arendustegevuste järjestatus prioriteetsuse alusel			
6	Teekaardis on olemas turvanõrkuste lahendamiseks vajalike arendustegevuste ühe aasta tegevuskava			
7	Teekaardis on olemas hinnang ettevõtja töötajate teadlikkusele küberturvalisuse riskidest			
7a	*Kui eelnev on jah* Hinnang ettevõtja töötajate teadlikkusele on ajakohane ja piisav			

2. Teekaardi kaardistuse skoop:

Skoop	Olemas	Kommentaar (vajadusel)
avalikust internetist potentsiaalsete rünnete sooritamiseks kasuliku informatsiooni kogumine ja tehniliste nõrkuste leidmine		
välisperimeeter ja avalikud veebilehed		
tulemüüri kasutus ja tulemüürireeglite ülevaatus		
kaugligipääsud – VPN, IPSEC tunnelid jm		
kontorite võrgud: tööjaamad ja serverid		
kontorite Wifi võrgud ja nende seadmed		
serverite võrgud ja haldusvõrgud		
serveri- ja seadmeruumide füüsilise turbe vaatlus		
riskianalüüsi ja taasteplaanide olemasolu ja ülevaatus		

vajadusel valvesüsteemid ja nende võrgud – läbipääsusüsteemid, videovalve		
vajadusel automaatikavõrgud – UPS-id, hooneautomaatika		

3. Teekaardi minimaalsed nõuded:

	Osa	**Jah**	**Ei**	**Kommentaar (vajadusel)**
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			
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			
8a	*Kui eelnev on jah:* Iga tähtsama leiu kohta on olemas järgmised detailid: • viide komponendile või süsteemile • probleemi kirjeldus • juhend probleemi esilekutsumiseks • hinnang probleemi tõsidusele • soovitused ja ettepanekud probleemi kõrvaldamiseks • CVSS skoor (kui võimalik)			
9	Ilmnenud probleemide koondtabel			
9a	*Kui 9. punkt on jah*: Koondtabelis on välja toodud soovituslik järjekord probleemide lahendamiseks			
9b	*Kui 9. punkt on jah*: Koondtabelis on antud hinnang probleemide lahendamise prioriteetsusele ja keerukusele			
10	Lühike tegevuskava, milliste tegevustega saab ettevõte 1 aasta jooksul kõige paremini punktis 9 nimetatud soovitusi ellu viia.			

Viited:

Toetuse andmise kord

5.4. Teekaart peab sisaldama:

5.4.1. ajakohast organisatsiooni küberturvalisuse taseme kaardistust, sh võrkude, tulemüürireeglite, kaugligipääsude, serverite võrkude ja haldusvõrkude, valvesüsteemide võrkude, automaatikavõrkude, serveri ja seadmeruumide füüsilise turbe võrkude, vajadusel valvesüsteemide võrkude ja automaatikavõrkude ülevaatust, riskianalüüside ülevaatust, hinnangut ettevõtja töötajate teadlikkusele küberturvalisuse riskidest ja ettepanekuid küberturvalisuse taseme tõstmiseks;

5.4.2. hinnangut leitud turvanõrkuste lahendamise prioriteetsusele ja arenduse keerukusele. Hinnang on piisava täpsusastmega sisendiks edasiste arendustegevuste elluviimiseks koostatava dokumentatsiooni ja tegevuse hinnastamiseks;

5.4.3. hinnangut punktis 2 nimetatud arendustegevuste läbiviimise kestusele, järjestatust ja ühe (1) aasta tegevuskava.

Juhis ettevõtte küberturvalisuse baastaseme hindamiseks ja Küberpöörde teekaardi koostamiseks

Versioon 1.0

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.

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.