Vabariigi Valitsuse 25. augusti 2011 korralduse nr 372
„Hädaolukorra „Ulatuslik küberrünnak“
lahendamise plaani kehtestamine“
lisa

Ulatusliku küberrünnaku hädaolukorra lahendamise plaan

1. Sissejuhatus

Ulatusliku küberrünnaku hädaolukorra lahendamise plaan (edaspidi *plaan*) sätestab hädaolukorra lahendamise korralduse ulatusliku küberrünnaku korral.

2. Peamiste plaani rakendusalaga seotud mõistete seletused

2.1. **Küberrünnak** on küberruumi vahenditega ja küberruumi vastu toimuv rünnak eesmärgiga peatada teenuste osutamine või vähendada nende käideldavust või rikkuda andmete terviklust või konfidentsiaalsust.

2.2. **Ulatuslik küberrünnak** on elutähtsa teenuse osutaja infosüsteemide või elutähtsa teenuse osutaja infosüsteemide tööks vajalike teiste asutuste või ettevõtjate (edaspidi *isik*) infosüsteemide vastu suunatud küberrünnak, millega osaliselt või täielikult katkeb elutähtsa teenuse toimepidevus või tekib reaalne oht elutähtsa teenuse toimepidevuse katkemisele või mille tõttu juhtub või võib potentsiaalselt juhtuda vähemalt üks järgmistest:

a) ohtu satub paljude inimeste elu või tervis;

b) tekib suur keskkonna- või varaline kahju ja sealhulgas füüsilisi purustusi kriitilisele infrastruktuurile;

c) tekib oluline mainekahju riigile;

d) ühiskonna majandusaktiivsuse oluline langus ja ühiskonnakorralduse destabiliseerumine.

2.3. **Küberruum** on arvutitel ja arvutisüsteemidel põhinev digitaalne ruum, mis toetab tänapäevase infoühiskonna toimimist ja koosneb peamiselt Interneti poolt võimaldatud tegevuskeskkondadest ja igapäevaste toimingute lihtsustamiseks loodud digitaalsetest andmekogudest.

2.4. **Hädaolukorra lahendamine** käesoleva plaani mõistes hõlmab tegevusi, mille eesmärk on esmajärjekorras kõrvaldada reaalne oht, taastada elutähtsa teenuse toimimine ja/või piirata ja/või vähendada ulatuslikust küberründest tingitud kahju.

3. Hädaolukorra lahendamise korraldus

Ulatusliku küberründe korral juhib hädaolukorra lahendamist Riigi Infosüsteemi Amet. Riigi Infosüsteemi Amet kaasab hädaolukorra lahendamisele isikuid, arvestades nende isikute pädevust ning volitusi.

4. Hädaolukorra lahendamise plaani rakendamine

4.1. Otsuse ulatusliku küberrünnaku hädaolukorra plaani rakendamise kohta teeb Riigi Infosüsteemi Ameti peadirektor tuginedes infoturbeintsidentide käsitlemise osakonna (edaspidi *CERT-EE*) poolt tehtud vormikohasele kirjalikule ettepanekule, kus muu hulgas on vajadusel arvestatud ekspertide arvamust;

4.2. Isik, kes on sattunud küberrünnaku alla, teavitab hädaolukorrast või hädaolukorra tekkimise vahetust ohust CERT-EE-d.

4.3. Teavitus sisaldab järgmisi andmeid:

4.3.1. sündmuse toimumise aeg (kuupäev, kellaaeg või ajavahemik);

4.3.2. sündmuse võimalikult täpne toimumiskoht;

4.3.3. sündmuse lühikirjeldus ning teadaolev või oletatav põhjus;

4.3.4. teadaolevad andmed hukkunute ja kannatanute kohta;

4.3.5. teadaolevad andmed elanike evakueerimise või selle vajaduse kohta;

4.3.6. teadaolevad andmed prognoositava kahju kohta varale ja keskkonnale (võimaluse korral rahalises väärtuses);

4.3.7. teadaolevad andmed prognoositava mõju kohta elutähtsate teenuste toimepidevusele (millised elutähtsad teenused on mõjutatud, mõjutatud isikute hulk);

4.3.8. millised isikud on hädaolukorrast või hädaolukorra tekkimise vahetust ohust teavitatud;

4.3.9. hädaolukorrast või hädaolukorra tekkimise vahetust ohust teavitamist vajavad teised isikud.

4.4. CERT-EE dokumenteerib küberrünnaku alla sattunud isiku teavituse.

4.5. Riigi Infosüsteemi Amet kaasab väljapoolt asutust eksperte eri tüüpi küberünnakute lahendamiseks.

4.6. Otsuse ulatusliku küberrünnaku hädaolukorra plaani rakendamise lõpetamise kohta teeb Riigi Infosüsteemi Ameti peadirektor, tuginedes CERT-EE tehtud ettepanekule.

4.7. CERT-EE koostab hiljemalt ühe kuu jooksul alates hädaolukorra plaani rakendamisest Riigi Infosüsteemi Ameti peadirektorile hädaolukorra raporti, mis sisaldab muu hulgas järgmisi andmeid:

4.7.1. hädaolukorra lühikirjeldus;

4.7.2. hädaolukorra lahendamist juhtiva asutuse või ametiisiku ning hädaolukorra lahendamiseks moodustatud juhtimisstruktuuride kontaktandmed;

4.7.3. hädaolukorra lahendamisele kaasatud asutused, isikud ja ressursid;

4.7.4. planeeritavad tegevused ja rakendatud abinõud

4.7.5. hädaolukorra lahendamisega seotud probleemid ja prognoos edaspidiseks

4.7.6. muudatused hädaolukorra lahendamise juhtimises või lahendamise juhi kontaktandmetes, hädaolukorra lahendamise aeg.

5. Hädaolukorra lahendamise juhtimisstruktuur

5.1. Riigi Infosüsteemi Amet moodustab ulatusliku küberrünnaku korral hädaolukorra lahendamise juhtimisstruktuuri.

5.2. Riigi Infosüsteemi Ameti moodustatud üleriigilise hädaolukorra lahendamise juhtimisstruktuuri kaasatakse:

5.2.1. ulatusliku küberrünnaku alla langenud isikuid;

5.2.2. elutähtsate teenuste toimepidevust korraldavaid asutusi;

5.2.3. teisi isikuid sõltuvalt rünnaku ulatusest ja mõjust;

5.2.4. eksperte;

5.2.5. vajadusel Prokuratuur, Politsei- ja Piirivalveamet ning Kaitsepolitseiamet.

6. Hädaolukorra lahendamisel osalevad isikud ja nende ülesanded

6.1. Hädaolukorra lahendamisel osalevad:

6.1.1. ulatusliku küberrünnaku alla langenud isikuid;

6.1.2. elutähtsa teenuse toimepidevust korraldav asutus;

6.1.3. Siseministeerium;

6.1.4. Riigi Infosüsteemi Amet.

6.2. Riigi Infosüsteemi Amet:

6.2.1. määrab hädaolukorra lahendamise juhtimisstruktuuri;

6.2.2. koordineerib hädaolukorra lahendamisega seotud isikute tegevusi;

6.2.3. omab ülevaadet hädaolukorra lahendamisel osalevate isikute ressursside kohta ning koordineerib nende kasutamist;

6.2.4. kogub ja analüüsib hädaolukorra lahendamiseks vajalikku teavet;

6.2.5. jälgib ja analüüsib hädaolukorra lahendamisega seotud sündmuste arengut;

6.2.6. koondab teadaolevad andmed prognoositava mõju kohta elutähtsate teenuste toimepidevusele;

6.2.7. korraldab hädaolukorra lahendamisega seotud isikute teabevahetust;

6.2.8. hindab vajadust kaasata rahvusvahelist abi ja vajadusel kaasab või teeb ettepaneku selle kaasamiseks.

6.3. Elutähtsa teenuse osutaja, kes on sattunud ulatusliku küberrünnaku alla:

6.3.1. teavitab hädaolukorrast elutähtsa teenuse toimpidevust korraldavat asutust;

6.3.2. teavitab hädaolukorrast punktis 4.3 sätestatud korras ja teavitab hädaolukorra lahendamiseks kasutusele võetud meetmetest ja tavaolukorra taastamisest Riigi Infosüsteemi Ametit;

6.3.3. rakendab oma toimepidevuse plaani ning taastab infosüsteemide töö.

6.4. Isikud, kes on vajalikud elutähtsa teenuse osutaja infosüsteemide tööks ja on sattunud küberrünnaku alla:

6.4.1. teavitavad hädaolukorrast (vt punkti 4.3), selle lahendamiseks kasutusele võetud meetmetest ja tavaolukorra taastamisest Riigi Infosüsteemi Ametit;

6.4.2. rakendavad oma toimepidevuse plaani ning taastavad infosüsteemide töö.

6.5. Elutähtsat teenuse toimepidevust korraldav asutus jälgib ja analüüsib hädaolukorra lahendamisega seotud sündmuste arengut.

6.6. Siseministeeriumi teabe- ja analüüsiosakond, olles saanud elutähtsa teenuse toimepidevust korraldavalt asutuselt teavituse ulatusliku küberründe kohta:

6.6.1. edastab teabe Riigi Infosüsteemi Ametile (kui teavituse esitaja ei ole Riigi Infosüsteemi Amet);

6.6.2. edastab teabe Vabariigi Valitsuse kriisikomisjonile ja kriisikomisjoni esimehe korraldusel teistele asjassepuutuvatele isikutele;

6.6.3. määrab ajavahemiku, kui tihti peab Riigi Infosüsteemi Ametile hädaolukorra lahendamise ajal teavet edastama.

6.7. Kaitseliidu küberkaitse üksus, olles saanud küberrünnaku alla sattunud elutähtsa teenuse osutajalt abipalve ulatusliku küberrünnaku lahendamise toetamiseks, aitab kaasa oma oskuste ja võimaluste piires hädaolukorra lahendamisele.

7. Avalikkuse teavitamise korraldus

7.1. Ulatusliku küberrünnaku korral koordineerib avalikkuse teavitamist hädaolukorra lahendamisest Riigi Infosüsteemi Amet.

7.2. Riigi Infosüsteemi Amet annab koostöös elutähtsa teenuse toimepidevust korraldavate asutustega avalikkusele juhiseid olukorras käitumiseks, et ennetada väärinformatsioonist tulenevaid võimalikke ohte.

7.3. Avalikkuse teavitamisel on vajalik kindlustada järgneva teabe kättesaadavus:

7.3.1. info rünnaku all olevatest e-teenustest, veebilehtedest jne;

7.3.2. info olukorra lahendamisega seotud asutustest ja isikutest;

7.3.3. käitumisjuhised olukorras tegutsemiseks;

7.3.4. võimaluse korral info küberründe asjaoludest;

7.3.5. teenuste taastamiseks plaanitavad tegevused.

8. Rahvusvahelise koostöö korraldus hädaolukorra lahendamisel

8.1. Hädaolukorra lahendamiseks vajaliku rahvusvahelise abi kaasamise õigus on Vabariigi Valitsusel, kes tugineb otsuse langetamisel Vabariigi Valitsuse kriisikomisjoni ettepanekule rahvusvahelise abi kaasamise osas.

8.2. Vabariigi Valitsus võib välislepingu alusel volitada Riigi Infosüsteemi Ametit taotlema hädaolukorra lahendamiseks vajalikku rahvusvahelist abi.

8.3. Rahvusvahelise abi taotlus esitatakse kas otse välisriigile või rahvusvahelisele organisatsioonile.

8.4. Rahvusvahelist koostööd hädaolukorra lahendamisel osalevate välisriikide, sealhulgas välisriikide välisesindustega Eesti Vabariigis ja rahvusvaheliste organisatsioonidega, sealhulgas nende esindustega Eesti Vabariigis korraldab Riigi Infosüsteemi Amet, teavitades rahvusvahelisest koostööst Majandus- ja Kommunikatsiooniministeeriumi ning Välisministeeriumi.

9. Kulude hüvitamise korraldus

9.1. Esmase kulude katteallikana nähakse ette hädaolukorra lahendamisel osalevate asutuste eelarvelised vahendid.

9.2. Vahendite mittepiisavusel või puudumisel esitatakse taotlus kulude katmiseks Vabariigi Valitsuse reservist vastavalt Vabariigi Valitsuse reservist raha eraldamise ja selle kasutamise korrale.