ÜKSIKASJALIK JUHENDMATERJAL CSIRTI ASUTAMISEKS

Tulemusdokument WP2006/5.1(CERT-D1/D2)

Sisukord

1 Kokkuvõte

Käesolevas dokumendis kirjeldatakse arvutiturbe juhtumitele reageerimise töörühma (CSIRT – *Computer Security Incident Response Team*) loomise kõiki olulisemaid aspekte – ärijuhtimist, protsesside juhtimist ja tehnilist külge. Käesolev dokument hõlmab ENISA 2006. aasta tööprogrammi peatükis 5.1 kirjeldatud kahte tulemusdokumenti:

- Käesolev dokument: *CERTi või samalaadsete asutuste loomise üksikasjaliku ülevaate (sh näited) kirjalik aruanne.* (**CERT-D1**)
- 12. peatükk ja lisadokumendid: T*egevuskava liigendatud esitus, mis võimaldab seda hõlpsasti ellu viia.* (**CERT-D2**)

2 Õiguslik märkus

3 Tänuavaldused

ENISA tänab kõiki asutusi ja üksikisikuid, kes aitasid selle dokumendi loomisele kaasa. Eriti tänulikud oleme järgmistele toetajatele:

- Henk Bronk, kelle nõustamisel valmis käesoleva dokumendi esimene versioon;
- CERT/CC ja eelkõige CSIRTi arendusrühm, kes andsid meie käsutusse äärmiselt kasulikke materjale ning lisades leiduva näidiskursuse materjalid;
- GovCERT.NL ülevaate „*CERT-in-a-box*“ eest;
- TRANSITSi töörühm, kes andis meile lisas leiduva näidiskursuse materjali;
- tehnikaosakonna turbepoliitika sektsioonis töötavad kolleegid, kes lisasid peatüki 6.6;
- kõik need inimesed, kes on selle dokumendi kriitilise pilguga üle vaadanud.

4 Sissejuhatus

Sidevõrkudest ja infosüsteemidest on saanud oluline tegur nii majanduse kui ka ühiskonna arengus. Informaatika ja võrkude loomine on muutumas samasuguseks üldlevinud kommunaalteenuseks kui elektri- või veevarustus.

Sidevõrkude ja infosüsteemide turvalisus, eelkõige nende kättesaadavus, on seetõttu ühiskonnas järjest aktuaalsem. Peamiseks mureallikaks on tähtsamaid infosüsteeme ohustavad probleemid, mis tulenevad süsteemide keerukusest, õnnetusjuhtumitest, vigadest ja rünnakutest Euroopa Liidu kodanike heaolu jaoks olulisi teenuseid osutavate füüsiliste infrastruktuuride vastu.

10. märtsil 2004 loodi Euroopa Võrgu- ja Infoturbe Amet (*European Network and Information Security Agency,* ENISA)[1]. Selle sammu eesmärk oli tagada ühenduse võrgu- ja infoturbe kõrge ja tõhus tase ning töötada Euroopa Liidu kodanike, tarbijate, ettevõtete ning avaliku sektori organisatsioonide jaoks välja võrgu- ja infoturbekultuur, mis omakorda aitaks kaasa siseturu sujuvale toimimisele.

Mitmed Euroopa turbeühendused (CERTid/CSIRTid, väärkasutuse töörühmad (*Abuse Team*) ja WARPid) on turvalisema Interneti nimel juba aastaid koostööd teinud. ENISA eesmärk on toetada selliste ühenduste püüdlusi, pakkudes teavet meetmetest, mis on võetud teenuse kvaliteedi vajaliku taseme tagamiseks. Lisaks kavatseb ENISA suurendada oma suutlikkust anda nõu ELi liikmesriikidele ja ELi asutustele asjakohaste turbeteenuste osas, mida pakutakse konkreetsetele IT-kasutajarühmadele. Seetõttu tegeleb uus töörühm 2005. aastal loodud ajutise koostöö ja tugirühma CERT tulemuste põhjal küsimustega, mis on seotud adekvaatsete turbeteenuste (“CERTi teenused”) osutamisega konkreetsetele kasutajatele (või nende kategooriatele või rühmadele).

ENISA toetab uute CSIRTide asutamist, avaldades käesoleva ENISA aruande *„Üksikasjalik lähenemine CSIRTi loomisele koos täiendava kontrollnimekirjaga”*, mis aitab teil luua oma CSIRT.

[1] Euroopa Parlamendi ja nõukogu 10. märtsi 2004. aasta määrus (EÜ) nr 460/2004 Euroopa Võrgu- ja Infoturbe Ameti loomise kohta. Euroopa Ühenduse amet on asutus, mille Euroopa Liit on loonud mõne väga konkreetse tehnilise, teadusliku või haldusalase ülesande täitmiseks ühenduse poliitikas ("esimese samba" valdkond).

4.1 Sihtrühm

Käesolev aruanne on suunatud eelkõige valitsusasutustele ja muudele organisatsioonidele, mis otsustavad luua CSIRTi, et kaitsta enda või oma sidusrühmade IT-infrastruktuure.

4.2 Selle dokumendi kasutamisest

Käesolev dokument annab ülevaate CSIRTi olemusest, turbetöörühma osutatavatest teenustest ja rühma loomiseks vajalikest sammudest. See peaks andma lugejale hea ja praktilise ülevaate CSIRTi loomise viisist, struktuurist ja sisust.

4. peatükk – *„Sissejuhatus“*
Käesoleva aruande sissejuhatus

5. peatükk – *„CSIRTi kavandamise ja loomise üldstrateegia“*
Esimeses punktis kirjeldatakse CSIRTi põhiolemust. Samuti antakse ülevaade erinevatest keskkondadest, kus CSIRTid saavad töötada, ja sellest, milliseid teenuseid CSIRT võib osutada.

6. peatükk – *„Äriplaani väljatöötamine“*
Selles peatükis kirjeldatakse loomisprotsessi ärijuhtimise seisukohalt.

7. peatükk – *„Äriplaani edendamine“*
Selles peatükis käsitletakse investeeringu põhjendust ja finantseerimisküsimusi.

8. peatükk – *„Tehniliste ja tööprotseduuride näited“*
Selles peatükis kirjeldatakse teabe hankimise ja turvabülletäänina vormistamise toiminguid. Samuti kirjeldatakse selles peatükis juhtumitöötluse töövoogu.

9. peatükk – *„CSIRTi koolitus“*
Selles peatükis antakse ülevaade saadaolevatest CSIRTi alase koolituse võimalustest. Näidiskursuse materjalid on toodud käesoleva dokumendi lisas.

10. peatükk – *„Harjutus: nõuande koostamine“*
See peatükk sisaldab harjutust, kuidas osutada üht põhilist CSIRTi teenust – koostada turva- või nõuandebülletääni.

12. peatükk – *„Projektikava kirjeldus“*
Selles peatükis käsitletakse koos käesoleva juhendiga pakutavat täiendavat projektikava (kontrollnimekirja). Kava on mõeldud käesolevas juhendis leiduvate soovituste kasutamise hõlbustamiseks.

4.3 Dokumendi peatükkide ülesehitus

Lugeja juhendamiseks algab iga peatükk CSIRTi loomise käigus seni tehtud toimingute kokkuvõttega. Need kokkuvõtted on välja toodud kastidena, näiteks:

Esimene toiming on nüüd tehtud.

Iga peatükk lõpeb selles käsitletud toimingute praktilise näitega. Käesoleva dokumendi näidetes kasutatud fiktiivne CSIRT on keskmise suurusega ettevõtte või asutuse väike sõltumatu CSIRT. Kokkuvõtte leiate lisast.

Fiktiivne CSIRT

5 CSIRTi kavandamise ja loomise üldstrateegia

Turbetöörühma ehk CSIRTi loomiseks on esmalt vaja täpset ettekujutust sellest, milliseid teenuseid töörühm saab oma kasutajatele ehk klientidele osutada. Asjakohaste teenuste õigeaegseks ja kvaliteetseks pakkumiseks tuleb mõista klientide vajadusi.

5.1 Mis on CSIRT?

CSIRT (Computer Security Incident Response Team) on töörühm, kes tegeleb arvutiturbe vahejuhtumitega. Kuna mõiste CERT on USA-s asutuse CERT Coordination Center (CERT/CC) poolt registreeritud, kasutatakse Euroopas selle asemel peamiselt mõistet CSIRT.
Samalaadseid arvutiturbega seotud töörühmi tähistatakse mitmesuguste suurtähtlühendite abil:

- CERT või CERT/CC (*Computer Emergency Response Team* / *Coordination Center*)
- CSIRT (*Computer Security Incident Response Team*)
- IRT (*Incident Response Team*)
- CIRT (*Computer Incident Response Team*)
- SERT (*Security Emergency Response Team*)

Esimene ulatuslikum ussviiruse puhang ülemaailmses IT-infrastruktuuris leidis aset 1980. aastate lõpus. Ussviiruse nimi oli Morris[2] ning see levis kiiresti, nakatades suure osa IT-süsteemidest üle kogu maailma.

See juhtum toimis omamoodi äratusena: äkitselt tunnetati vajadust süsteemiadministraatorite ja IT-juhtide vahelise koostöö järele, et selliste juhtumitega tegelda. Kuna aeg oli ülimalt oluline tegur, tuli IT-turbega seotud juhtumite käsitlemiseks kiiresti välja töötada senisest organiseeritum ja parema struktuuriga lähenemisviis. Nii asutas DARPA (Defence Advanced Research Projects Agency) juba mõni päev pärast Morrise juhtumit esimese CSIRTi: keskuse nimega CERT Coordination Center (CERT/CC[3]), mis asus Pittsburghis (Pennsylvanias) Carnegie Melloni ülikooli juures.

See mudel võeti peagi kasutusele ka Euroopas ja 1992. aastal käivitas Hollandi haridusasutustele mõeldud võrguteenuste pakkuja SURFnet Euroopa esimese CSIRTi, mis sai nimeks SURFnet-CERT[4]. Järgnes arvukalt uusi töörühmi ja praegu sisaldab ENISA veebilehel asuv loend *Inventory of CERT activities in Europe*[5] juba enam kui 100 Euroopas tegutsevat töörühma.

Aja jooksul on CERTide tegevusvaldkond laienenud – enam pole tegemist pelgalt reageerimisüksusega, vaid täielikku turbeteenuste komplekti pakkuva töörühmaga, kes osutab ka ennetusteenuseid (hoiatused, turbenõuanded, koolitus ja turbehaldusteenused). Mõiste „CERT“ osutus peagi ebapiisavaks. Seetõttu võeti 1990.

[2] Lisateavet ussviiruse Morris kohta: http://en.wikipedia.org/wiki/Morris_worm

[3] CERT-CC, http://www.cert.org

[4] SURFnet-CERT: http://cert.surfnet.nl/

[5] ENISA Inventory: http://www.enisa.europa.eu/cert_inventory/

aastate lõpus kasutusele uus mõiste „CSIRT“. Praegu kasutatakse mõlemat mõistet (CERT ja CSIRT) sünonüümidena, ehkki CSIRT on täpsem.

5.1.1 Mõiste *„constituency“*

CSIRTi kliendibaasi tähistatakse inglise keeles CSIRTidega seotud ringkondades omaks võetud mõistega „constituency“. Üksikklienti tähistab inglise keeles mõiste „constituent“, klientide rühma seevastu mõiste „constituents“.

5.1.2 CSIRTi määratlus

CSIRT on IT-turbespetsialistidest koosnev töörühm, kelle peamine tegevusvaldkond on arvutiturbega seotud juhtumitele reageerimine. Töörühm osutab teenuseid, mis on vajalikud nii nende juhtumite lahendamiseks kui ka klientide toetamiseks turberikkumistest taastumisel.

Riskide leevendamiseks ja nõutavate vastuste arvu vähendamiseks osutab enamik CSIRTe klientidele ka ennetus- ja koolitusteenuseid. Lisaks annavad töörühmad nõu kasutuseloleva tarkvara ja riistvara haavatavuse kohta ning teavitavad kasutajaid nõrkadele kohtadele suunatud rünnakuvõimalustest ja viirustest. Nii saavad kliendid oma süsteeme kiiresti paigata ja värskendada. Võimalike teenuste täieliku loendi leiate peatükist *5.2 Võimalikud teenused*.

5.1.3 CSIRTi olemasolu eelised

IT-turbetöörühma olemasolu aitab organisatsioonil suuremaid vahejuhtumeid ennetada või nende tagajärgi leevendada ning oma väärtuslikku vara kaitsta.

Lisaks on sel muidki eeliseid:

- organisatsioonis on IT-turbega seotud küsimused keskselt koordineeritud (kontaktpunkt);
- IT-juhtumite keskne ja spetsialiseeritud käsitsemine ning juhtumitele reageerimine;
- turbeprobleemide tekkimisel on spetsialistid koha käepärast, aidates kasutajatel probleemide tagajärgedega kiiresti toime tulla;
- õigusküsimustega tegelemine ja asitõendite säilitamine hagi korral;
- turbevaldkonna arengute jälgimine;
- klientide omavahelise IT-turbe alase koostöö edendamine (teadlikkuse suurendamine).

Fiktiivne CSIRT (toiming 0)
CSIRTi olemuse mõistmine Näidis-CSIRT peab teenindama keskmise suurusega asutust, kus töötab kuni 200 inimest. Asutusel on oma IT-osakond ja veel kaks harukontorit samas riigis. Infotehnoloogial on ettevõtte jaoks oluline roll, kuna seda kasutatakse ettevõttesisese suhtluse, andmevõrgu ja ööpäev läbi töötava e-äri jaoks. Asutusel on oma võrk ja liiasühendus Internetiga kahe erineva Interneti-teenuse pakkuja kaudu.

5.1.4 Erinevate CSIRTi keskkondade kirjeldus

Oleme ära teinud esimese toimingu 1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda. >> Järgmiseks tuleb vastata küsimusele „Millisele sektorile CSIRTi teenuseid pakutakse?“

Nagu iga muu ettevõtte asutamisel, on ka CSIRTi loomisel oluline saada selge ülevaade sellest, kes moodustavad töörühma kliendibaasi ja mis tüüpi keskkonna jaoks CSIRTi teenuseid arendama hakatakse. Praegu tehakse vahet järgmistel valdkondadel, järjestus on tähestikuline:

- Akadeemilise sektori CSIRT
- Asutusesisene CSIRT
- CIP/CIIP sektori CSIRT
- Kaubanduse CSIRT
- Riiklik CSIRT
- Sõjandussektori CSIRT
- Tootja CSIRT
- Valitsussektori CSIRT
- Väikeste ja keskmise suurusega ettevõtete sektori CSIRT

Akadeemilise sektori CSIRT
Fookus
Akadeemilise sektori CSIRTid osutavad teenuseid akadeemilistele ja haridusasutustele (nt ülikoolidele või teaduskeskustele) ning õppelinnakute Interneti-keskkondadele.

Kliendibaas
Seda tüüpi CSIRTi kliendibaasi moodustavad enamasti ülikoolide õppejõud ja õppurid.

Asutusesisene CSIRT
Fookus
Asutusesisene CSIRT osutab teenuseid ainult töörühma majutavale asutusele. See kirjeldab pigem töörühma toimimist kui sektorit. Asutusesisesed CSIRTid on olemas näiteks paljudel telekommunikatsioonieettevõtetel ja pankadel. Enamasti pole sellistel CSIRTidel avalikult juurdepääsetavat veebisaiti.

Kliendibaas
Töörühma majutava asutuse töötajad ja IT-osakond.

CIP/CIIP sektori CSIRT
Fookus

Selle sektori CSIRTide tähelepanu on üldjuhul suunatud kriitilise tähtsusega teabe kaitsele (CIP – *Critical Information Protection*) ja/või kriitilise tähtsusega teabe ja infrastruktuuri kaitsele (CIIP – *Critical Information and Infrastructure Protection*). Enamasti teeb eriotstarbeline CSIRT tihedat koostööd riikliku CIIP-osakonnaga. Sellise töörühma tegevus hõlmab kõiki riigi kriitilise tähtsusega IT-sektoreid ja kaitseb vastava riigi kodanikke.

Kliendibaas
Riigiasutused; kriitilise tähtsusega IT-ettevõtted; kodanikud.

Kaubanduse CSIRT
Fookus
Kaubanduse CSIRT osutab klientidele teenuseid ärilisel põhimõttel. Interneti-teenuse pakkujate puhul osutab CSIRT lõppkasutajatest klientidele (sissehelistusühenduse või ADSL-i kasutajatele) enamasti väärkasutust käsitlevaid teenuseid ja professionaalsetele kasutajatele CSIRTi teenuseid.

Kliendibaas
Kaubanduse CSIRTid osutavad tavaliselt teenuseid klientidele, kes teenuste eest maksavad.

Riiklik CSIRT
Fookus
Tervet riiki hõlmava fookusega CSIRT, mis on käsitletav riigi IT-turbe kontaktpunktina. Mõnel juhul toimib valitsussektori CSIRT ühtlasi ka riikliku kontaktpunktina (nt Ühendkuningriigis UNIRAS).

Kliendibaas
Sellist tüüpi CSIRTil pole üldjuhul otseseid kliente, sest riiklik CSIRT täidab üksnes kogu riigi vahendaja rolli.

Sõjandussektori CSIRT
Fookus
Selle sektori CSIRTid osutavad sõjaväeorganisatsioonidele kaitseotstarbelise IT-infrastruktuuri vajadustega seotud teenuseid.

Kliendibaas
Sõjaväeasutuste või nendega lähedalt seotud juriidiliste isikute (nt kaitseministeeriumi) töötajad.

Tootja CSIRT
Fookus
Tootja CSIRT on enamasti keskendunud tootja spetsiifiliste toodete toetamisele. Tavaliselt on CSIRTi eesmärgiks arendada ja pakkuda lahendusi haavatavuse kõrvaldamiseks ja vigade võimaliku negatiivse mõju leevendamiseks.

Kliendibaas
Toodete omanikud

Valitsussektori CSIRT
Fookus
Valitsussektori CSIRT osutab teenuseid riigiasutustele ja mõnes riigis ka kodanikele.

Kliendibaas
Valitsus ja valitsusega seotud asutused; mõnes riigis osutatakse teavitusteenuseid ka kodanikele (nt Belgias, Ungaris, Hollandis, Ühendkuningriigis ja Saksamaal).

Väikeste ja keskmise suurusega ettevõtete (SME) sektori CSIRT
Fookus
Ise oma tööd korraldav CSIRT, mis osutab teenuseid oma ärivaldkonnale või muudele sarnastele kasutajarühmadele.

Kliendibaas
Selliste CSIRTide kliendid võivad olla väikesed ja keskmise suurusega ettevõtted ning nende töötajad või teatud kindlad huvirühmad, nt kohalik linnade ja valdade ühendus.

Nagu riiklikke CSIRTe käsitlevas lõigus kirjeldatud, on võimalik, et üks töörühm teenindab rohkem kui ühte sektorit. See mõjutab näiteks kliendibaasi ja tema vajaduste analüüsi.

Fiktiivne CSIRT (toiming 1)
Alustamine Algfaasis kavandatakse uus CSIRT ettevõttesisesena, mis osutab teenuseid töörühma majutavale ettevõttele, kohalikule IT-osakonnale ja töötajatele. Samuti toetab ja koordineerib CSIRT eri harukontorite IT-turbega seotud juhtumite käsitlemist.

5.2 Teenused, mida CSIRT võib osutada

Oleme ära teinud kaks esimest toimingut

1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda.
2. Millisele sektorile uus töörühm teenuseid osutab?

>> Järgmiseks tuleb vastata küsimusele, *milliseid teenuseid klientidele osutada.*

CSIRT võib osutada mitmesuguseid teenuseid, kuid siiani pole ükski CSIRT tegelnud kõigi võimalike teenuste pakkumisega. Seetõttu on sobiva teenustekomplekti valimine äärmiselt oluline otsus. Allpool leiate põgusa ülevaate kõigist teadaolevatest CSIRTide osutatavatest teenustest vastavalt CERT/CC avaldatud käsiraamatule „Handbook for CSIRTs“[6].

[6] CERT/CC CSIRTide käsiraamat http://www.cert.org/archive/pdf/csirt-handbook.pdf

Reaktiivsed teenused	**Proaktiivsed teenused**	**Artefaktide käsitlemine**
• **Teated ja hoiatused** • **Juhtumi käsitlemine** • **Juhtumianalüüs** • **Juhtumitele reageerimise tugiteenused** • **Juhtumitele reageerimise koordineerimine** • Kohapealne reageerimine juhtumitele • Haavatavuste käsitlemine • Haavatavuste analüüs • Haavatavustele reageerimine • Haavatavustele reageerimise koordineerimine	• **Teadaanded** • Tehnoloogiaseire • Turbeauditid või -hindamised • Turvalisuse konfigureerimine ja haldamine • Turbetööriistade väljatöötamine • Sissetungituvastusteenused • Turbealase teabe levitamine	• *Artefaktianalüüs* • *Artefaktidele reageerimine* • *Artefaktidele reageerimise koordineerimine* ***Turbekvaliteedi juhtimine*** • *Riskianalüüs* • *Majandustegevuse jätkamine ja tõrgete kõrvaldamine* • *Turbealane nõustamine* • *Teadlikkuse suurendamine* • *Haridus/koolitus* • *Tootehindamine või -sertifitseerimine*

Joonis 1 CSIRTi teenuste loend, CERT/CC[7]

Põhiteenused (paksus kirjas): eristatakse reaktiivseid ja proaktiivseid teenuseid. Proaktiivsete teenuste eesmärk on juhtumite ärahoidmine teadlikkuse suurendamise ja koolituse abil, reaktiivsed teenused seevastu on suunatud juhtumite käsitlemisele ja kahjude leevendamisele.

Artefaktide käsitlemine hõlmab kõigi selliste arvutisüsteemist leitud failide või objektide analüüsimist, mis võivad olla kaasatud pahatahtlikesse toimingutesse (nt uss- ja muude viiruste, skriptide, Trooja hobuste jms järelmõjud jne). Samuti hõlmab see valdkond saadud teabe käsitlemist ja levitamist tootjatele ja muudele huvitatud osapooltele, vältimaks õelvara edasist levikut ja leevendamaks riske.

Turbe- ja kvaliteedijuhtimisteenused on pikaajaliste eesmärkidega teenused, mis hõlmavad mitmesuguseid nõustamis- ja koolitusmeetmeid.

CSIRTi teenuste üksikasjaliku selgituse leiate lisast.

Kliendibaasi jaoks õigete teenuste valimine on töörühma loomisel oluline etapp, mida käsitletakse täpsemalt peatükis *6.1 Finantsmudeli määratlemine*.

Enamik CSIRTe alustab tegevust kliendibaasile teadete ja hoiatuste levitamise, teadaannete edastamise ning juhtumite käsitlemise teenuste osutamisega. Üldjuhul

[7] CSIRT teenuste loend, CERT/CC: http://www.cert.org/csirts/services.html

aitavad need põhiteenused kliendibaasi silmis tõsta töörühma profiili ja silmatorkavust ning neid käsitletakse enamasti tegeliku lisandväärtusena.

Sageli tasub alustada väikese rühma klientidega, osutada neile teatud katseaja jooksul põhiteenuseid ja küsida seejärel tagasisidet.
Pilootprojekti kaasatud kasutajad, kellele teenused pakuvad huvi, annavad üldjuhul konstruktiivset tagasisidet ja aitavad välja töötada kliendibaasi jaoks kohandatud teenuseid.

Fiktiivne CSIRT (toiming 2)
Õigete teenuste valimine Projekti algetapis otsustatakse, et uus CSIRT keskendub peamiselt asutuse töötajatele teatud põhiteenuste pakkumisele. Otsustatakse, et pärast katseetappi kaalutakse pakutavate teenuste valiku laiendamist ja valikusse võidakse lisada ka teatud turbehaldusteenused. Selle otsuse tegemisel lähtutakse pilootprojektis osalenud klientidelt saadud tagasisidest ja kvaliteedikontrolli osakonnaga tehtud tihedast koostööst.

5.3 Kliendibaasi analüüs ja missiooni sõnastamine

Oleme ära teinud kolm esimest toimingut

1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda.
2. Millisele sektorile uus töörühm teenuseid osutab?
3. Mis liiki teenuseid võib CSIRT oma kliendibaasile osutada?

>> Järgmiseks tuleb vastata küsimusele*, milline lähenemisviis tuleks CSIRTi alustamiseks valida.*

Järgmise sammuna tuleb põhjalikumalt analüüsida kliendibaasi, pidades silmas eelkõige sobivate sidekanalite valimist:

- klientidega sidepidamise võimaluste määratlemine;
- missiooni sõnastamine;
- realistliku juurutamis-/projektikava koostamine;
- CSIRTi teenuste määratlemine;
- organisatsioonilise struktuuri määratlemine;
- infoturbepoliitika määratlemine;
- sobivate töötajate palkamine;
- CSIRTi kontori ärakasutamine;
- muude CSIRTide ja võimalike riiklike algatustega koostöövõimaluste uurimine.

Neid toiminguid kirjeldatakse järgmistes lõikudes üksikasjalikumalt ning neid võib kasutada äriplaani ja projektikava koostamisel.

5.3.1 Kliendibaasiga sidepidamise võimalused

Nagu eespool öeldud, on äärmiselt oluline tunda nii kliendibaasi vajadusi kui ka omaenda suhtlusstrateegiat, sealhulgas seda, millised sidekanalid on klientidele teabe pakkumiseks kõige sobivamad.

Juhtimisteoorias tuntakse mitut võimalikku moodust, kuidas sihtrühma analüüsida. Käesolevas dokumendis kirjeldatakse neist kahte: SWOT- ja PEST-analüüsi.

SWOT-analüüs
SWOT-analüüs on strateegiate kavandamise vahend, mille abil hinnatakse projekti või äriettevõttega kaasnevaid või mõnes muus otsustamist nõudvas olukorras esinevaid tugevusi, nõrkusi, võimalusi ja ohtusid (**S**trengths, **W**eaknesses, **O**pportunities, **T**hreats). Selle analüüsimeetodi töötas välja Albert Humphrey, kes juhtis 1960. ja 1970. aastatel Stanfordi ülikoolis vastavat uurimisprojekti, kasutades Fortune 500 ettevõtete andmeid.[8]

Tugevus	**Nõrkus**
Võimalused	**Ohud**

Joonis 2 SWOT-analüüs

[8] SWOT-analüüsi kirjeldus Wikipedias: http://en.wikipedia.org/wiki/SWOT_analysis

PEST-analüüs

PEST-analüüs on kliendibaasi teine oluline analüüsivahend. Selle meetodi abil saab ülevaate CSIRTi töökeskkonna poliitilistest (**P**olitical), majanduslikest (**E**conomic), sotsiaalsetest (**S**ocio-cultural) ja tehnoloogilistest (**T**echnological) teguritest. PEST-analüüs aitab määratleda, kas kava on ikka keskkonnaga kooskõlas ning ilmselt võimaldab ka vältida valedel eeldustel põhinevaid otsuseid.

Poliitiline	**Majanduslik**
• Ökoloogilised/keskkonnaküsimused • Siseturu praegused õigusaktid • Tulevased õigusaktid • Euroopa/rahvusvahelised õigusaktid • Reguleerivad asutused ja protsessid • Riiklikud poliitikad • Valitsuse ametiaeg ja muutused • Kaubanduspoliitika • Rahastamine, toetused ja algatused • Siseturu mõju- ja surverühmitused • Rahvusvahelised surverühmitused	• Siseturu majanduslik olukord • Siseturu majanduse suundumused • Majanduse olukord ja suundumused teistes riikides • Üldised maksuküsimused • Toodet ja teenuste eriomased maksud • Hooaja-/ilmaküsimused • Turu- ja kaubandustsüklid • Konkreetse tegevusvaldkonna tegurid • Turustamisliinid ja levitussuundumused • Kliente/lõppkasutajaid suunavad tegurid • Intressid ja vahetuskursid
Sotsiaalne	**Tehnoloogiline**
• Elustiili suundumused • Demograafia • Tarbijate tõekspidamised ja arvamused • Ajakirjanduse seisukohad • Seadusalased muudatused, mis avaldavad mõju sotsiaalsetele teguritele • Kaubamärgi, ettevõtte, tehnoloogia kuvand • Tarbijate ostuharjumused • Mood ja eeskujud • Olulisemad sündmused ja mõjuallikad • Ostuvõimalused ja -suundumused • Rahvuslikud/usulised tegurid • Reklaam ja avalikkuse teavitamine	• Konkureeriva tehnoloogia väljatöötamine • Uurimistöö rahastamine • Seostuvad/sõltuvad tehnoloogiad • Asendustehnoloogia/-lahendused • Tehnoloogia küpsus • Tootmisküpsus ja -võimsus • Teave ja kommunikatsioon • Tarbijate ostumehhanismid/-tehnoloogia • Tehnoloogiaga seotud õigusaktid • Uuenduspotentsiaal • Juurdepääs tehnoloogiale, litsentsimine, patendid • Intellektuaalse omandi küsimused

Joonis 3 PEST-analüüsi mudel

PEST-analüüsi üksikasjaliku kirjelduse leiate Wikipediast[9].

Mõlemad meetodid annavad kliendibaasi vajadustest mitmekülgse struktureeritud ülevaate. Tulemused täiendavad äriettepanekut ja aitavad seega kaasa CSIRTi loomiseks vajalike vahendite saamiseks.

Sidekanalid

Analüüsi tuleb kindlasti kaasata võimalikud side- ja teabelevitusviisid („Kuidas kliendibaasiga suhelda?“).

[9] PEST-analüüsi kirjeldus Wikipedias: http://en.wikipedia.org/wiki/PEST_analysis

Võimalusel tuleks kaaluda regulaarset silmast-silma kohtumist klientidega. On tõestatud, et sellised kokkusaamised muudavad koostöö hõlpsamaks. Kui mõlemad pooled on koostööst huvitatud, aitavad kohtumised muuta töörühma ja klientide vahelisi suhteid avatumaks.

Enamasti on CSIRTide käsutuses hulk mitmesuguseid sidekanaleid. Järgmised sidekanalid on end praktikas tõestanud ja nende kasutamist tasuks kaaluda:

- avalik veebisait;
- veebisaidil leiduv suletud ala, kuhu pääsevad ainult liikmed;
- veebivormid juhtumitest teatamiseks;
- postitusloendid;
- isikupärastatud meilisõnumid;
- telefon/faks;
- SMS-sõnumid;
- „vanamoodsad“ paberkirjad;
- kuu- või aastaaruanded.

Lisaks e-posti, veebivormide, telefoni ja faksi kasutamisele juhtumite käsitlemise hõlbustamiseks (juhtumiteadete vastuvõtmiseks klientidelt, töö koordineerimiseks teiste meeskondadega või kuriteo ohvrile toe ja tagasiside pakkumiseks) avaldab enamik CSIRTe avalikult kättesaadaval veebisaidil ja postitusloendites turbenõuandeid.

! Võimalusel tuleks teavet levitada turvalisel viisil. Meilisõnumid saab näiteks PGP-krüpteeringut kasutades digitaalselt allkirjastada ning juhtumitega seotud tundliku loomuga andmed tuleks alati saata krüptitud kujul.

Lisateavet leiate peatükist *8.5 Saadaolevad CSIRTi tööriistad*. Vt ka *RFC2350*[10] peatükki *2.3*.

Fiktiivne CSIRT (toiming 3a)

Kliendibaasi ja sobivate sidekanalite analüüsi koostamine

Ajurünnak, kus osalesid teatud võtmeisikud juhtkonnast ja kliendibaasist, andis piisavalt lähteandmeid SWOT-analüüsi jaoks. Jõuti järeldusele, et klientide seas valitseb vajadus põhiteenuste järele:

- teated ja hoiatused;
- juhtumite käsitlemine (analüüs, reageerimistugi ja reageerimise koordineerimine);
- teadaanded.

Teabe levitamine peab olema hästi korraldatud, et teave jõuaks võimalikult suure osani kliendibaasist. Seetõttu võeti vastu otsus, et teated, hoiatused ja teadaanded (turbenõuannete kujul) avaldatakse nii vastaval veebisaidil kui ka postitusloendi kaudu levitades. CSIRT kasutab juhtumiteadete vastuvõtmiseks e-posti, telefoni ja faksi. Järgmises etapis kavatsetakse kasutusele võtta ühtne veebivorm.

[10] http://www.ietf.org/rfc/rfc2350.txt

SWOT-analüüsi näidise leiate järgmiselt lehelt.

Tugevus • Ettevõttes on olemas teatud teadmisi. • Kava on ettevõttele meeltmööda ja on olemas koostöövalmidus • Juhtkonna moraalne ja rahaline tugi	**Nõrkus** • Osakonnad ja harukontorid ei suhtle eriti omavahel • IT-juhtumite osas puudub koordinatsioon • Palju „väikesi osakondi“
Võimalused • Tohutu hulk struktureerimata teavet haavatavuse kohta • Tungiv vajadus teabe koordineerimise järele • Juhtumitest tingitud kahju vähendamine • Arvukalt lahtisi otsi IT-turbe osas • Töötajate IT-turbe alane koolitamine	**Ohud** • Raha pole kuigi palju saadaval • Töötajaid napib • Suured ootused • Kultuur

Joonis 4 SWOT-analüüsi näidis

5.3.2 Missiooni sõnastamine

Pärast kliendibaasi CSIRTi teenustega seotud vajaduste ja soovide analüüsimist tuleks koostada esialgne missiooni kirjeldus.

Missiooni kirjelduses antakse ülevaade asutuse peamisest funktsioonist ühiskonnas, lähtudes sellest, milliseid tooteid ja teenuseid see kliendibaasile pakub. Selle abil saab selgelt edasi anda uue CSIRTi olemuse ja funktsiooni.

Missiooni kirjeldus võiks olla kompaktne, kuid mitte liiga napisõnaline, kuna enamasti ei muudeta selle sõnastust mitme aasta jooksul.

Näiteid tegutsevate CSIRTide missiooni kirjeldustest:

„<CSIRTi nimi> pakub oma <klientidele (määratlege oma kliendibaas)> teavet ja abi proaktiivsete meetmete kasutuselevõtul, et vähendada arvutiturbega seotud juhtumite ohtu ning reageerida asetleidvatele juhtumitele.“

„<Kliendibaasile> IT-alaste turbejuhtumite ärahoidmise ja neile reageerimisega seotud abi osutamine“[11]
Missiooni kirjeldus on töörühma loomisel äärmiselt oluline ja vajalik etapp. Üksikasjalikuma kirjelduse selle kohta, millist teavet CSIRT peaks avaldama, leiate dokumendi *RFC2350*[12] peatükist *2.1*.

Fiktiivne CSIRT (toiming 3b)
Fiktiivse CSIRTi juhtkond on koostanud järgmise missiooni kirjelduse: *„Fiktiivne CSIRT pakub töörühma majutava ettevõtte töötajatele teavet ja abi proaktiivsete meetmete kasutuselevõtul, vähendamaks arvutiturbega seotud juhtumite ohtu ning reageerimaks sellistele juhtumitele, kui neid siiski esineb.“* Sellega väljendab fiktiivne CSIRT selgelt, et tegemist on asutusesisese CSIRTiga, mille põhitegevus seisneb IT-turbega seotud probleemide lahendamises.

[11] Govcert.nl'i missiooni kirjeldus: http://www.govcert.nl

[12] http://www.ietf.org/rfc/rfc2350.txt

6 Äriplaani väljatöötamine

Oleme ära teinud järgmised toimingud.

1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda.
2. Millisele sektorile uus töörühm teenuseid osutab?
3. Mis liiki teenuseid võib CSIRT oma kliendibaasile osutada?
4. Keskkonna ja kliendibaasi analüüsimine.
5. Missiooni sõnastamine.

>> Järgmiseks tuleb määratleda äriplaan.

Kuna analüüsi tulemus annab teile hea ülevaate kliendibaasi vajadustest ja (eeldatavatest) nõrkustest, kasutatakse seda järgmise etapi lähtekohana.

6.1 Finantsmudeli määratlemine

Pärast analüüsi on alustamiseks valitud paar põhiteenust. Järgmiseks tuleks mõelda finantsmudeli peale – millised teenuste osutamise parameetrid oleksid ühtaegu nii sobivad kui ka tasuvad.

Täiuslikus maailmas kohandataks rahalised vahendid kliendibaasi vajadustele, kuid tegelikus elus tuleb osutatavate teenuste valik viia kooskõlla olemasoleva eelarvega. Seega on realistlikum alustada rahaliste küsimuste planeerimisest.

6.1.1 Kulumudel

Kulusid mõjutab kaks põhilist tegurit – tööaeg ning töölevõetavate töötajate arv (ja kvaliteet). Kas juhtumitele reageerimise ja tehnilise toe teenuseid tuleb osutada ööpäev läbi või piisab sellest, kui neid osutatakse tööajal?

Sõltuvalt soovitud kättesaadavusest ja kontoriseadmetest (kas oleks näiteks võimalik ka kodust töötada?) võib olla hea mõte töötada väljakutse- või ajapõhise töögraafiku järgi.

Üks võimalus on osutada tööajal nii proaktiivseid kui ka reaktiivseid teenuseid. Väljaspool tööaega osutaks valves olev töötaja aga ainult piiratud teenuseid, näiteks väga tõsiste õnnetuste või juhtumite korral.

Teine võimalus on teha rahvusvahelist koostööd teiste CSIRTi meeskondadega. Nn „päikest järgiva“ mudeli alusel toimivaid koostöö näiteid leidub juba päris mitu. Euroopa ja Ameerika töörühmade koostöö on näiteks osutunud mõlemale poolele kasulikuks ning hõlbustab üksteise võimsuse ärakasutamist. Sun Microsystemsi CSIRTil näiteks on harukontoreid mitmes ajavööndis üle kogu maailma (kõik harukontorid on siiski sama CSIRTi liikmed) ja selleks, et teenuseid saaks osutada ööpäev läbi, antakse töökohustusi omavahel pidevalt üle. Nii on võimalik kulusid kokku hoida – iga töörühm töötab ainult oma ajavööndi tavalisel tööajal, kuid teenindab ühtlasi ka seda osa maailmast, kus on parajasti öö.

Kliendibaasi ööpäevaringsete teenuste vajadust tuleks kindlasti analüüsida väga hoolikalt. Öösel pole näiteks eriti mõtet teateid ja hoiatusi avaldada, kuna adressaadid loevad neid alles hommikul. Teenuse vajamise ja soovimise vaheline piir on sageli üsna peen, kuid just tööaeg mõjutab väga olulisel määral nii vajaminevate töötajate arvu kui ka tööks nõutavaid ruume ja seadmeid ning seega ka kulumudelit.

6.1.2 Tulumudel

Kui kuludest on ülevaade olemas, tasub järgmiseks mõelda võimalikele tulumudelitele – kuidas kavandatud teenuseid finantseerida. Järgnevas antakse ülevaade mõnest võimalusest.

Olemasolevate ressursside kasutamine
Alati on hea hinnata seda, millised ressursid on ettevõtte teistes osades juba olemas. Kas ettevõttes (näiteks olemasolevas IT-osakonnas) töötab juba sobivaid inimesi, kellel on olemas nii nõutav taust kui ka vajalikud oskused? Arvatavasti saab juhtkonnaga kokku leppida võimalustes kasutada samu töötajaid algetapis ka CSIRTi jaoks. Samuti on võimalik, et need töötajad saavad CSIRTid ajutiselt abistada.

Liikmemaks
Teine võimalus on teenuseid klientidele müüa näiteks kord aastas või kvartalis tasutava liikmemaksu eest. Lisateenuste (nt nõustamisteenuste või turbeauditite) eest saaks tasuda vastava teenuse kasutamisel.

Veel üks võimalus: (asutusesisesele) kliendibaasile osutatakse teenuseid tasuta, kuid väliskliendid peavad teenuste eest maksma. Samuti võib kaaluda nõuannete ja teabebülletäänide avaldamist avalikul veebisaidil, jättes üksikasjalikuma või täpsema teabe ainult liikmetele mõeldud jaotisse.

Praktikas on tõestatud, et CSIRTi teenuste tellimine on finantseerimisel abiks siiski ainult piiratud ulatuses, eriti projekti algusjärgus. Töötajate ja seadmetega on seotud kindlad põhikulud, mis tuleb maksta ette. Nende kulude katmine CSIRTi teenuste müümise kaudu on keeruline ja kasumiläveni jõudmine nõuab väga üksikasjalikku finantsanalüüsi.

Toetused
Kindlasti võiks kaaluda võimalust taotleda projekti jaoks riiklikku (või mõne riigiasutuse kaudu eraldatavat) toetust, kuna IT-turbega seotud projektide jaoks on toetused tänapäeval saadaval paljudes riikides. Näiteks võiks pöörduda siseministeeriumi poole.

Muidugi on võimalik erinevaid mudeleid omavahel kombineerida.

6.2 Organisatsioonilise struktuuri määratlemine

CSIRTi jaoks sobiv organisatsiooniline struktuur sõltub suures osas töörühma majutava asutuse struktuurist ja kliendibaasist. Samuti sõltub see ekspertide püsiva või ajutise värbamise võimalusest.

Tüüpilises CSIRTis on töörühmas määratletud järgmised rollid.

Üldine
- Üldjuht

Töötajad
- Juhataja
- Raamatupidaja
- Suhtlusnõustaja
- Juriidiline nõustaja

Tehnikameeskond
- Tehnikameeskonna juht
- CSIRTi tehnikud, kes osutavad CSIRTi teenuseid
- Uurijad

Välisnõustajad
- Palgatakse vajaduse korral

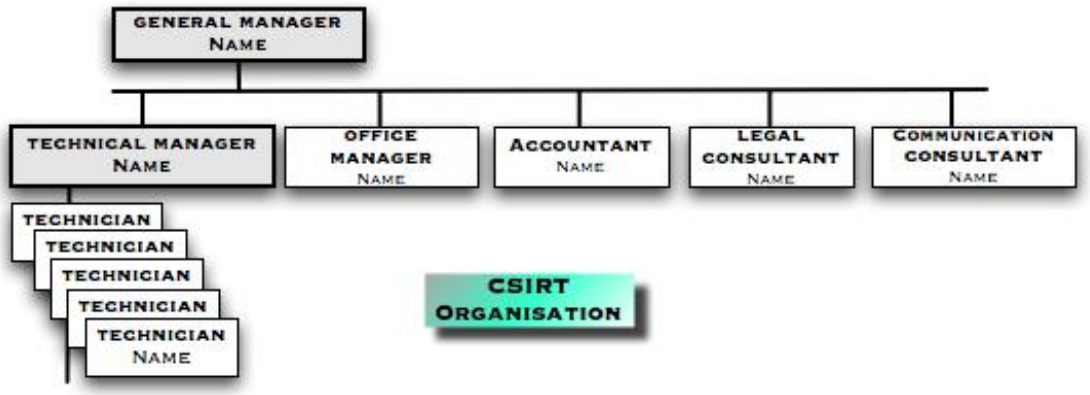
Õigusasjatundja kaasamine on eriti kasulik CSIRTi loomise algjärgus. See on küll kulukas, kuid pikemas perspektiivis hoiab kokku aega ja aitab vältida võimalikke õiguslikke probleeme.

Kui kliendibaas hõlmab väga erineva teadmiste ja oskuste tasemega inimesi või kui CSIRT leiab ajakirjanduses ohtralt kajastamist, on hea kaasata meeskonda ka suhtlusekspert. Need spetsialistid saavad keskenduda sellele, kuidas selgitada keerulisi tehnilisi probleeme klientidele või meediapartneritele arusaadavamas keeles. Lisaks saab suhtlusekspert anda tehnikutele edasi klientidelt saadud tagasisidet, toimides kahe rühma vahel vahendaja ja suhtekorraldajana.

Järgnevalt on toodud mõni näide reaalselt tegutsevates CSIRTides kasutatavatest organisatsioonimudelitest.

6.2.1 Sõltumatu ärimudel

CSIRT tegutseb omaette sõltumatu asutusena, millel on oma juhtkond ja töötajad.

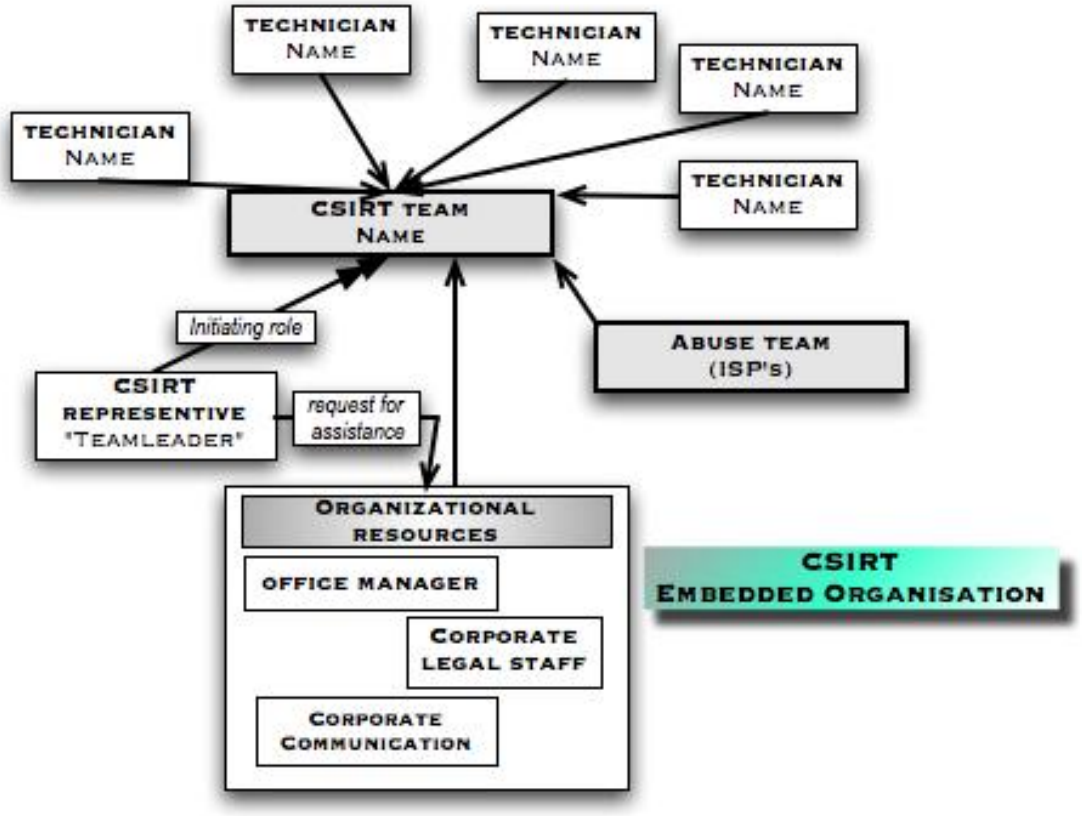


Joonis 5 Sõltumatu ärimudel

6.2.2 Integreeritud mudel

Seda mudelit võib kasutada juhul, kui CSIRTi kavatsetakse luua olemasoleva asutuse raames – näiteks juba olemasoleva IT-osakonna põhjal. CSIRTi juhib meeskonnajuht, kes vastutab CSIRTi tegevuse eest. Meeskonnajuht kutsub juhtumite lahendamisel või CSIRTi tegevustega töötamisel kohale vajalikud tehnikud. Kui vaja läheb spetsialisti abi, võib meeskonnajuht asutuse teistelt töötajatelt abi paluda.

Seda mudelit saab vastavalt vajadusele ka konkreetse olukordade jaoks kohandada. Sel juhul eraldatakse meeskonnale teatud kindel arv täistööajaga töötajaid. Interneti-teenuse pakkuja väärkasutusosakond näiteks vajab kindlasti vähemalt ühte või (enamikul juhtudel) mitut täistööajaga töötajat.

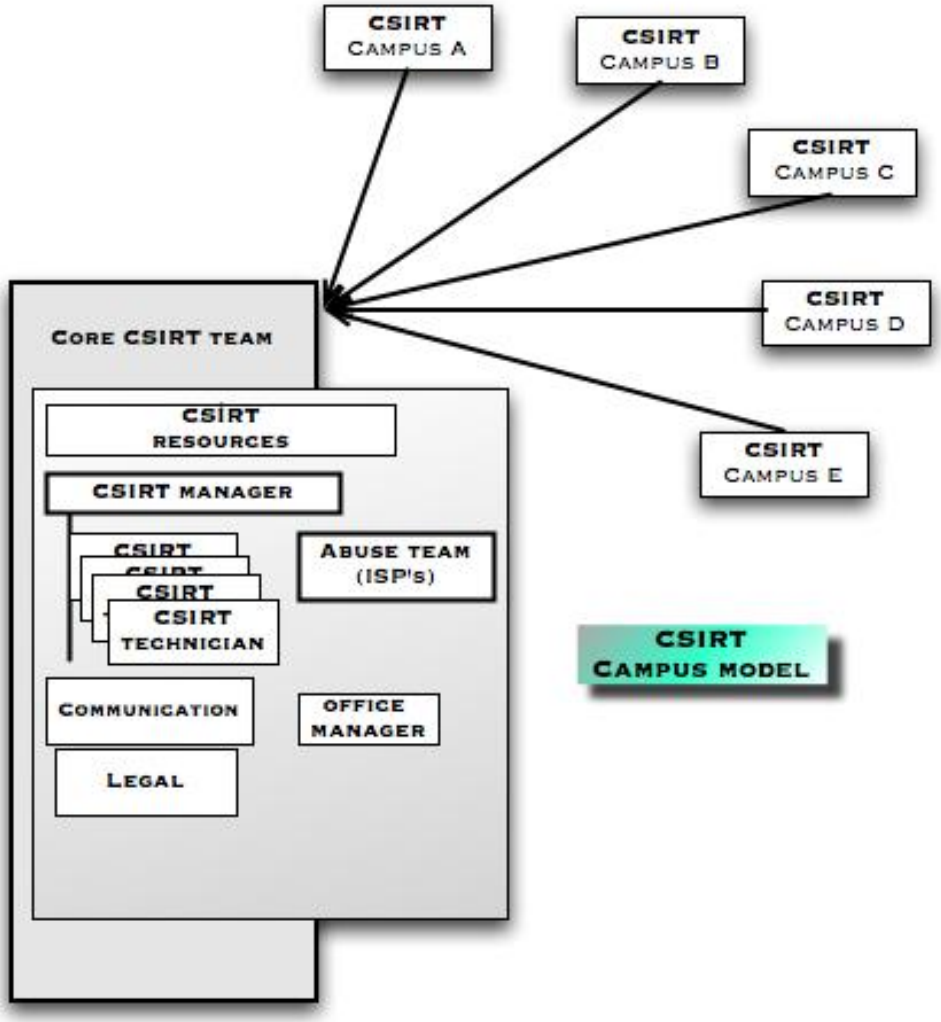


Joonis 6 Organisatsiooni integreeritud mudel

6.2.3 Õppelinnaku mudel

Õppelinnaku mudel – nagu nimestki näha – on enamasti kasutusel akadeemiliste ja teadustööga seotud CSIRTides. Enamik akadeemilisi ja teadustööga tegelevaid organisatsioone koosneb erinevates asukohtades asuvatest ülikoolidest ja õppelinnakutest, mis on hajutatud suurema piirkonna või koguni terve riigi peale (näiteks NREN-id ehk riigisisesed teadustöövõrgud). Üldjuhul on need organisatsioonid üksteisest sõltumatud ja sageli on igas organisatsioonis oma CSIRT. Need CSIRTid on enamasti korraldatud põhi-CSIRTi ümber (ühtse „vihmavarju“ alla). Põhi-CSIRT koordineerib kõigi CSIRTide tööd ja on ainus kontaktpunkt välismaailmaga. Enamikul juhtudel osutab põhi-CSIRT lisaks asjakohasele õppelinnaku CSIRTile juhtumiteabe edastamisele ka CSIRTi põhiteenuseid.

Mõni CSIRT osutab CSIRTi põhiteenuseid vaheldumisi teiste õppelinnaku CSIRTidega. Nii on põhi-CSIRTi kantavad kulud madalamad.



Joonis 7 Õppelinnaku mudel

6.2.4 Vabatahtlik mudel

See organisatsioonimudel kirjeldab üksteisele (ja teistele) nõuannete ja tugiteenuste pakkumiseks ühte koondunud vabatahtlike (spetsialistide) rühma. Tegemist on üsna lõdvalt seotud rühmaga, mille tegevus sõltub suuresti osalejate motiveeritusest.

Selle mudeli on omaks võtnud näiteks WARPi kogukond[13].

6.3 Sobivate töötajate palkamine

Kui osutatavate teenuste valiku ja tugiteenuste taseme osas on otsusele jõutud ja sobiv organisatsioonimudel valitud, tuleb järgmise sammuna ette võtta piisava arvu selle töö jaoks kvalifitseeritud töötajate otsimine.

Ehkki konkreetseid arve on käesolevas dokumendis peaaegu võimatu välja pakkuda, võib vajaliku arvu tehnikute väljaselgitamisel abi olla järgmistest põhitõdedest.

- Kahe põhiteenuse osutamiseks (nõustamisbülletäänide levitamiseks ja juhtumite käsitlemiseks) läheb vaja vähemalt **4** täistööajaga töötajat.
- Tööajal täielikku teenustekomplekti pakkuva CSIRTi jaoks ja süsteemide haldamiseks vajatakse vähemalt **6–8** täistööajaga töötajat.
- Ööpäev läbi täiskomplekti teenuseid osutavas töörühmas (kaks vahetust väljaspool tööaega) on vaja vähemalt **12** täistööajaga töötajat.

Need arvud on välja arvestatud varuga, võttes arvesse puudumisi haiguse tõttu, puhkepäevi jms. Samuti tuleks läbi vaadata kohalikud kollektiivlepingud. On võimalik, et väljaspool tavatööaega töötavatele inimestele tuleb maksta lisatasu, mis toob kaasa lisakulusid.

[13] WARPi algatus: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Järgnevalt antakse ülevaade CSIRTi tehnikaspetsialistide peamistest pädevusnõuetest.

Tehniliste töötajate ametijuhendi üldpunktid:

Isikuomadused

- Paindlik, loominguline ja hea meeskonnatöötaja
- Hea analüüsivõime
- Oskus selgitada keerulisi tehnilisi probleeme lihtsas sõnastuses
- Hea arusaam konfidentsiaalsusest ja protseduurieeskirjade järgimisest
- Head korraldamisoskused
- Stressitaluvus
- Head suhtlemis- ja kirjutamisoskused
- Eelarvamusteta ja õppimisvalmis

Tehnilised oskused

- Laialdased teadmised Interneti-tehnoloogiast ja protokollidest
- Linuxi ja Unixi süsteemide tundmine (sõltuvalt kliendibaasi kasutatavatest seadmetest)
- Windowsi süsteemide tundmine (sõltuvalt kliendibaasi kasutatavatest seadmetest)
- Võrguinfrastruktuuriseadmete (marsruuterid, kommutaatorid, DNS, puhverserverid, meiliserverid jne) tundmine
- Interneti-rakenduste (SMTP, HTTP(s), FTP, telnet, SSH jne) tundmine
- Turbeohtude (DDoS, andmepüük, moonutamine, nuuskimine jne) tundmine
- Teadmised riskianalüüsist ja selle praktikas juurutamisest

Täiendavad punktid

- Nõus töötama ööpäev läbi või väljakutsepõhiselt (sõltuvalt teenusemudelist)
- Läbitava vahemaa pikkus (kontoris töötamine hädaolukorras; töölesõitmisele kuluv aeg)
- Haridustase
- IT-turbe alal töötamise kogemus

Fiktiivne CSIRT (toiming 4)

Äriplaani määratlemine

Finantsmudel

Kuna ettevõttel on ööpäev läbi töötav e-äri ja samuti ööpäev läbi töötav IT-osakond, on jõutud otsusele osutada tööajal täiskomplekti teenuseid ning väljaspool tööaega töötada väljakutsepõhiselt. Kliendibaasile osutatakse teenuseid tasuta, kuid projekti piloot- ja hindamisetapis analüüsitakse võimalust osutada teenuseid ka välisklientidele.

Tulumudel

Projekti algusjärgus ja pilootetapi ajal finantseeritakse CSIRTi tegevust seda majutava ettevõtte kaudu. Piloot- ja hindamisetapis arutatakse täiendavaid finantseerimisvõimalusi (sh võimalust müüa teenuseid välisklientidele).

Organisatsioonimudel

Kuna töörühma majutav asutus on väikeettevõte, on valitud integreeritud mudel.
Tööajal osutab kolmest töötajast koosnev personal põhiteenuseid (turbenõuannete levitamine ja juhtumite käsitlemine/koordineerimine).

Vajalike oskustega inimesed on ettevõtte IT-osakonnas juba olemas. Selle osakonnaga sõlmitakse kokkulepe, mille alusel saab uus CSIRT vajaduse korral ajutist abi taotleda. Lisaks saab kasutada IT-osakonna väljakutsete alusel töötavaid tehnikuid.
CSIRTi põhimeeskonnas hakkab töötama neli täiskohaga inimest; lisaks annab CSIRT tööd veel viiele inimesele. Üks neist on nõus töötama erinevates vahetustes.

Töötajad
CSIRTi meeskonnajuhil on kogemusi IT-turbe vallas. Samuti on ta töötanud esimese ja teise taseme tugiteenuseid osutavas asutuses ja paindliku kriisihalduse valdkonnas. Ülejäänud kolm meeskonnaliiget on turbespetsialistid. Osalise tööajaga töötavad CSIRTi liikmed, kelle põhitöökoht on IT-osakonnas, on ettevõtte infrastruktuuri osas oma ala spetsialistid.

6.4 Kontori kasutamine ja seadmed

Kuna see, milliseid seadmeid töörühmal vaja läheb, kuidas olemasolevat kontoriruumi kõige paremini ära kasutada ning kuidas seda füüsiliselt turvata, on väga lai teema, ei saa seda käesolevas dokumendis väga põhjalikult käsitleda. Selles peatükis antakse neist punktidest lühike ülevaade.

Füüsilise turvalisuse kohta leiate lisateavet järgmistelt veebilehtedelt:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

Hoone turvamine
Kuna CSIRTid töötlevad enamasti väga tundliku loomuga teavet, on hea mõte anda kontroll kontori füüsilise turvalisuse üle sama töörühma kätte. Loomulikult sõltub see olemasolevatest ehitistest ja infrastruktuurist ning töörühma majutava ettevõtte olemasolevast turbepoliitikast.

Riigiasutused näiteks kasutavad klassifitseerimisskeeme ja konfidentsiaalse teabe käsitsemisel kehtivad ranged piirangud. Uurige kindlasti välja, millised reeglid või poliitikad teie ettevõttes või asutuses kehtivad.

Uus CSIRT peab kehtivate reeglite, poliitikate ja muude juriidiliste küsimuste osas teabe hankimiseks üldjuhul sõltuma koostööst töörühma majutava asutusega.

Kõigi vajalike seadmete ja turvameetmete põhjalik kirjeldus jääb käesoleva dokumendi ulatusest välja. Järgmine loend annab siiski ülevaate CSIRTi põhivajadustest.

Hoone üldreeglid
- Hoidke hoonele juurdepääs kontrolli all.
- Võimalusel tagage, et CSIRTi kontorisse pääseksid ainult CSIRTi töötajad.
- Pange kontoriruumidesse ja sissepääsude juurde turvakaamerad.
- Hoidke konfidentsiaalseid dokumente seifis või lukustatavas kapis.
- Kasutage turvalisi IT-süsteeme.

IT-seadmete üldreeglid
- Kasutage selliseid seadmeid, mille hooldamisega saavad hakkama ettevõtte enda töötajad.
- Turvake kõik süsteemid.
- Paigake ja värskendage kõik süsteemid enne nende Internetti ühendamist.
- Kasutage turbetarkvara (tulemüürid, mitmesugused viirusetõrjerakendused, nuhkvaratõrje jne).

Sidekanalite haldamine
- Avalik veebisait
- Veebisaidil leiduv suletud ala, kuhu pääsevad ainult liikmed
- Veebivormid juhtumitest teatamiseks
- E-post (PGP / GPG / S/MIME tugi)
- Postitusloenditarkvara
- Klientidele kättesaadav spetsiaalne telefoninumber:
    - telefon
    - faks
    - SMS

Kirjejälgimissüsteemid
- Kontaktteabe andmebaas (meeskonnaliikmete, teiste meeskondade jne teave)
- CRM-tööriistad
- Juhtumite käsitlemise süsteem

Kasutage ettevõttes kasutusel olevat kujundust kohe töörühma algusest peale:
- meilisõnumite ja nõustamisbülletäänide standardpaigutus;
- „vanamoodsad“ paberkirjad;
- kuu- või aastaaruanded;
- juhtumitest teatamise vorm.

Muu
- Mõelge välja, millised täiendavaid sidevõimalusi saaks kasutada rünnakute korral
- Kavandage Interneti-ühenduse varuvõimalused

Konkreetsete CSIRTi tööriistade kohta leiate lisateavet peatükist *8.5 Saadaolevad CSIRTi tööriistad*.

6.5 Infoturbepoliitika väljatöötamine

Sõltuvalt sellest, mis tüüpi CSIRT teil on, peate kohandama ka oma infoturbepoliitika. Lisaks soovitud operatsiooni- ja haldusprotsesside ja -protseduuride kirjeldamisele peab selline poliitika olema kooskõlas õigusaktide ja standarditega, seda eriti CSIRTi vastutuse osas. CSIRT peab üldjuhul täitma riiklikke õigusnorme, mis on sageli kasutusele võetud Euroopa õigusaktide (enamasti direktiivide) ja muude rahvusvaheliste lepingute kontekstis. Standardid pole küll tingimata otseselt siduvad, kuid õigusnormid võivad need teha kohustuslikuks või soovituslikuks.

Järgmises loendis on ära toodud osa võimalikest õigusaktidest ja poliitikatest.

Riiklikud
- Mitmesugused õigusaktid, mis käsitlevad infotehnoloogiat, telekommunikatsiooni ja meediat
- Andmekaitset ja privaatsust käsitlevad õigusaktid
- Andmete säilitamist käsitlevad õigusaktid
- Rahandust, raamatupidamist ja ettevõtete juhtimist käsitlevad õigusaktid
- Ettevõtete juhtimise ja IT-juhtimise tegevusjuhendid

Euroopa Liit
- Direktiiv elektrooniliste allkirjade kohta (1999/93/EÜ)
- Direktiivid andmekaitse (1995/46/EÜ) ja elektroonilise side privaatsuse (2002/58/EÜ) kohta
- Direktiivid elektrooniliste sidevõrkude ja -teenuste kohta (2002/19/EÜ – 2002/22/EÜ)
- Direktiivid äriseaduste kohta (nt 8. äriseaduste direktiiv)

Rahvusvahelised
- Basel II leping (eriti tegevusriski juhtimise osas)
- Euroopa Nõukogu küberkuritegevuse konventsioon
- Euroopa Nõukogu inimõiguste konventsioon (artikkel 8, mis käsitleb privaatsust)
- Rahvusvaheline raamatupidamisstandard (IAS; see standard reguleerib teatud määral ka IT juhtimist)

Standardid
- Briti standard BS 7799 (infoturve)
- Rahvusvahelised standardid ISO2700x (infoturbe haldussüsteemid)
- Saksamaa IT-Grundschutzbuch, Prantsusmaa EBIOS ja muud riiklikud variandid

Kui soovite kindlaks teha, kas teie CSIRT tegutseb kooskõlas riiklike ja rahvusvaheliste õigusaktidega, küsige nõu juristilt.

Töörühma teabekäitluspoliitikat koostades tuleks mõelda järgmistele põhiküsimustele:

- Kuidas saabuv teave märgistatakse või liigitatakse?
- Kuidas teavet töödeldakse (eriti monopoolsuse osas)?

- Milliseid kaalutlusi võetakse arvesse teabe avaldamisel, eriti juhul, kui juhtumitega seotud teavet edastatakse teistele meeskondadele või saitidele?
- Kas teabetöötluse osas tuleb arvesse võtta ka mingeid juriidilisi asjaolusid?
- Kas teil on olemas poliitika krüptograafia kasutamise kohta monopoolsuse ja tervikluse kaitsmiseks arhiivides ja/või andmesides, eelkõige e-posti osas?
- Kas see poliitika hõlmab võimalikke juriidilisi piirtingimusi (nt võtmehoiustust või sundkorras dekrüptimist kohtuasjade korral)?

Fiktiivne CSIRT (toiming 5)
Kontoriseadmed ja asukoht Kuna töörühma majutaval ettevõttel on füüsiline turvalisus juba tõhusalt paigas, ei pea uus CSIRT selle pärast muretsema. Tegevuse koordineerimiseks hädaolukorras seatakse sisse nn staap. Krüptimismaterjalide ja tundliku loomuga dokumentide hoidmiseks ostetakse seif. Sisse on seatud eraldi telefoniliin, sh kommutaator, mis võimaldab kasutada sama telefoninumbrit tööajal infoliini teenindamiseks ja väljaspool tööaega väljakutseid ootava töötaja mobiiltelefoni ühendamiseks. CSIRTiga seotud teabe avaldamiseks võib kasutada ka ettevõtte veebisaiti ja olemasolevaid seadmeid. Sisse seatakse postitusloend, mille piiratud juurdepääsuga osa on mõeldud suhtlemiseks meeskonnaliikmete vahel ja teiste meeskondadega. Andmebaasis hoitakse kõigi töötajate kontaktandmeid; kontaktandmete väljaprinti hoitakse seifis. **Eeskirjad** Kuna CSIRT on integreeritud ettevõttega, millel on infoturbepoliitika juba olemas, on vastav poliitika ettevõtte juristi abiga välja töötatud ka CSIRTi jaoks.

6.6 Muude CSIRTide ja võimalike riiklike algatustega koostöövõimaluste uurimine

Muude CSIRTi algatuste olemasolu ja nendevahelise koostöö vajadust on käesolevas dokumendis juba paar korda mainitud. CSIRTide kogukonnaga vajalike kontaktide loomiseks tasub teiste CSIRTidega ühendust võtta võimalikult aegsasti. Enamasti on teised CSIRTid meelsasti nõus uusi töörühmi alguses abistama.

Teiste kohalike või rahvusvaheliste CSIRTide otsimisega saab algust teha ENISA veebilehel jaotises *Inventory of CERT activities in Europe*[14].

Kui soovite CSIRTi teabe jaoks sobiva allika otsimisel abi, pöörduge ENISA CSIRTi asjatundjate poole:

CERT-Relations@enisa.europa.eu

[14] ENISA veebileht: http://www.enisa.europa.eu/cert_inventory/

Järgnevalt antakse ülevaade CSIRTi kogukondade tegevustest. Põhjalikuma kirjelduse ja lisateavet leiate mainitud ENISA veebilehe jaotisest (*Inventory of CERT activities in Europe;* edaspidi viidates *Inventory)*.

Euroopa CSIRTi algatus

TF-CSIRT[15]
TF-CSIRTi rakkerühm edendab Euroopa arvutiturbe juhtumitele reageerimise töörühmade (CSIRTide) vahelist koostööd. Selle rakkerühma peamised eesmärgid on kogemuste ja teadmiste vahetamiseks sobiva foorumi pakkumine, Euroopa CSIRTide kogukonna jaoks pilootteenuste loomine ning uute CSIRTide asutamisele kaasaaitamine.

Rakkerühma peamised eesmärgid on järgmised:
- kogemuste ja teadmiste vahetamiseks sobiva foorumi pakkumine;
- Euroopa CSIRTide kogukonna jaoks pilootteenuste loomine;
- turbejuhtumitele reageerimiseks ühtsete standardite ja protseduuride edendamine;
- uute CSIRTide asutamisele kaasaaitamine ja CSIRTide töötajate koolitamine;
- TF-CSIRTi tegevus hõlmab Euroopat ja lähiümbrust (kooskõlas TERENA tehnikakomitee poolt 15. septembril 2004 vastu võetud tingimustega).

Ülemaailmne CSIRTi algatus

FIRST[16]
FIRST on juhtumitele reageerimise valdkonnas üldtunnustatud globaalne liider. FIRSTiga liitumisel saavad juhtumitele reageerimise töörühmad turbejuhtumitele reageerida senisest tõhusamalt – nii reaktiivselt kui ka proaktiivselt.

FIRST koondab paljude riigiasutuste, ettevõtete ja haridusasutuste arvutiturbe juhtumitele reageerimise töörühmi. FIRSTi eesmärkide seas on juhtumite ärahoidmise alase koostöö ja koordineerimise edendamine, juhtumitele kiire reageerimise ergutamine ning teabevahetuse toetamine nii liikmete seas kui ka kogu ühiskonnas.

Lisaks usaldusvõrgustikule, mille FIRST on globaalses juhtumitele reageerimise kogukonnas loonud, pakub FIRST ka lisaväärtusteenuseid.

Fiktiivne CSIRT (toiming 6)
Koostöövõimalustega tutvumine ENISA veebilehe jaotise *Inventory* kaudu õnnestus kiiresti üles leida mitu samas riigis tegutsevat CSIRTi, kellega võeti ühendust. Vastne meeskonnajuht korraldas ühe CSIRTiga kokkusaamise. Lisaks koosolekul osalemisele saadi teavet riiklike CSIRTide tegevuste kohta. Koosolek osutus erakordselt kasulikuks: koguti näiteid töömeetodite kohta ja saadi abi mitmelt muult töörühmalt.

[15] TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

[16] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

7 Äriplaani edendamine

Seni oleme ära teinud järgmised toimingud.

1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda.
2. Millisele sektorile uus töörühm teenuseid osutab?
3. Mis liiki teenuseid võib CSIRT oma kliendibaasile osutada?
4. Keskkonna ja kliendibaasi analüüsimine.
5. Missiooni sõnastamine.
6. Äriplaani väljatöötamine
    a. Finantsmudeli määratlemine
    b. Organisatsioonilise struktuuri määratlemine
    c. Töötajate palkamine
    d. Kontori kasutuselevõtt ja varustamine
    e. Infoturbepoliitika väljatöötamine
    f. Koostööpartnerite otsimine

>> Järgmiseks tuleb eelkirjeldatud punktidest kokku panna projektikava ja pihta hakata!

Projekti määratlemist võiks alustada investeeringupõhjenduse koostamisest. Investeeringupõhjendust kasutatakse projektikava aluspõhjana, kuid seda saab kasutada ka juhtkonnalt toetuse küsimiseks ja eelarve või muude ressursside hankimiseks.

Hea mõte on juhtkonda oma tegevusega pidevalt kursis hoida, et IT-turbeprobleemide alane teadlikkus püsiks kõrgel ja tagaks CSIRTile ettevõtte pideva toe.

Investeeringupõhjenduse koostamist alustatakse probleemide ja võimaluste analüüsimisega. Seda tehakse analüüsimudeli abil (vt peatükki *5.3 Kliendibaasi analüüs*). Seejärel tuleks sisse seada kontaktid potentsiaalse kliendibaasiga.

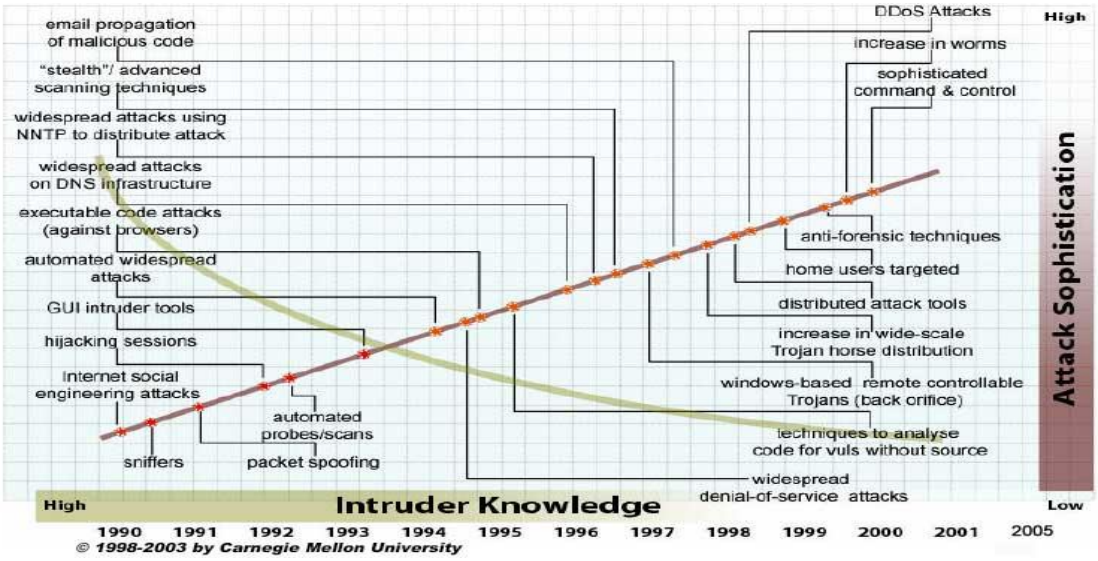
Nagu eespool kirjeldatud, on CSIRTi asutamisel vaja päris põhjalikult järele mõelda. Eespool mainitud materjalid tuleks kohandada CSIRTi muutuvatele vajadustele.

Juhtkonnale aruannete esitamisel tasub lähtuda võimalikult värsketest materjalidest, tuginedes näiteks hiljutistele ajakirjanduses või Internetis avaldatud artiklitele ja põhjendades, miks on CSIRTi teenused ja juhtumite asutusesisene koordineerimine ettevõtte põhivahendite turvamiseks üliolulised. Samuti tuleb selgitada, et stabiilseks äritegevuseks on vaja IT-turbega seotud asjaolude järjepidevat toetamist, seda eriti juhul, kui IT-l on ettevõtte või asutuse tegevuses oluline roll.

(Seda aitab hästi illustreerida Bruce Schneieri tuntud mõtteavaldus: *„Turvalisus on protsess, mitte toode[17]!“)*

Turbeprobleeme illustreerib ka järgmine CERT/CC koostatud tuntud graafik:

[17] Bruce Schneier: http://www.schneier.com/



Joonis 8 Sissetungijate teadmised võrreldes rünnaku keerukusega (allikas: CERT-CC[18])

Graafikul on kujutatud IT-turbe alased suundumused. See näitab ilmekalt, kuidas aina keerukamate rünnakute sooritamiseks on vaja aina vähem teadmisi.

Mainida tasub ka seda, et haavatavuste parandamiseks vajalike tarkvarauuenduste kättesaadavuse ja neid haavatavusi ära kasutavate rünnakute alguse vahele jääv aeg on aina lühem:

Paik -> ärakasutamine		**Levimiskiirus**	
Nimda:	11 kuud	Code red:	Päevad
Slammer:	6 kuud	Nimda:	Tunnid
Nachi:	5 kuud	Slammer:	Minutid
Blaster:	3 nädalat		
Witty:	1 päev (!)		

Esitlusel on abiks ka juhtumite kohta kogutud andmetest, võimalikest parendusviisidest ja saadud õppetundide kirjeldusest.

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

7.1 Äriplaanid ja juhtkonnale esitatavad põhjendused

Juhtkonnale tehtav ettekanne, mis hõlmab ainult CSIRTi propageerimist, pole omaette võetuna veel piisav investeeringupõhjendus, ent kui ettekanne teha õigesti, tagab see enamasti CSIRTile juhtkonna toe. Investeeringupõhjendust ei peaks siiski pidama ainult juhtimisharjutuseks, vaid seda tuleks kasutada ka töörühma ja kliendibaasiga suhtlemisel. Investeeringupõhjenduse mõiste võib küll tunduda liiga kommertslik ja CSIRTi tavategevusest eemalseisev, kuid CSIRTi asutamisel aitab see tegevuskava täpsemini välja töötada.

Hea investeeringupõhjenduse koostamisel võib abi olla järgmistele küsimustele antud vastustest. (Toodud näited on hüpoteetilised ja neid kasutatakse ainult illustreerival otstarbel. Tegelikud vastused sõltuvad suures osas tegelikest oludest.)

- Milles seisneb probleem?
- Mida soovite kliendibaasi osas saavutada?
- Mis juhtub siis, kui te ei võta midagi ette?
- Mis juhtub siis, kui võtate midagi ette?
- Kui palju see kõik maksma läheb?
- Mida sellega saavutatakse?
- Millal alustada ja millal see valmis saab?

Milles seisneb probleem?
Enamasti tekib CSIRTi asutamise mõte siis, kui IT-turbest on saanud ettevõtte või asutuse põhitegevuse oluline osa ja kui IT-turbega seotud juhtumid hakkavad ohustama äritegevust. Sel juhul saab turbeprobleemide leevendamisest osa tavalisest äritegevusest.

Enamikul ettevõtetel ja asutustel on olemas tavaline tugiteenuste osakond või infoliin, kuid üldjuhul ei suuda need osakonnad turbejuhtumeid piisava tõsidusega käsitleda ega ole nii struktureeritud kui vaja. Turbejuhtumite valdkond nõuab töötajatelt enamasti erioskusi ja süvenemist. Struktureeritum lähenemine on kasulik ka selle poolest, et see leevendab ohte äritegevusele ja ettevõtte kahjusid.

Probleem on sageli selles, et osakonnad ei koordineeri oma tööd piisavalt ning juhtumite käsitlemiseks ei kasutata olemasolevaid teadmisi, ehkki see võiks ära hoida nii edaspidiseid probleeme kui ka potentsiaalseid rahalisi kaotusi ja/või asutuse maine kahjustamist.

Millised on kliendibaasiga seotud eesmärgid?
Nagu eespool juba kirjeldatud, tegeleb CSIRTi kliendibaasi teenindamisega, aidates neil lahendada IT-turbega seotud juhtumeid ja probleeme. Täiendavaks eesmärgiks võib kindlasti pidada IT-turbega seotud teadlikkuse üldist tõstmist.

Üldise turbeteadlikkuse õhkkonnas võetakse proaktiivsed ja ennetavad meetmed kasutusele algusest peale, mis omakorda aitab tegevuskulusid kokku hoida.

Ettevõttes või asutuses sellise koostööd ja üldist üksteise abistamist soodustava õhkkonna edendamine aitab enamasti kaasa ka üleüldiselt tõhusamale tööle.

Mis juhtub siis, kui ette ei võeta midagi?

IT-turbe struktureerimata käsitlemine võib kaasa tuua senisest suuremaid probleeme, kahjustades muu hulgas ka asutuse mainet. Samuti võib olla tulemuseks rahaline kahju ja õiguslikud probleemid.

Mis juhtub siis, kui midagi ette võtta?

Tõstetakse teadlikkust turbeprobleemide esinemisest. See aitab probleeme tõhusamalt lahendada ja edaspidiseid kaotusi ära hoida.

Kui palju see kõik maksma läheb?

Sõltuvalt organisatsioonimudelist hõlmavad ettevõtmisega seotud kulud CSIRTi liikmete ja asutuse töötajate palku ning seadmete, tööriistade ja tarkvaralitsentside ostmist.

Mida sellega saavutatakse?

Sõltuvalt ettevõtte tegevusvaldkonnast ja varasematest kahjudest muudab CSIRTi olemasolu tegevuse ja turbekäitumise läbipaistvamaks, mis omakorda aitab kaitsta ettevõtte põhivahendeid.

Milline on ajakava?

Projektikava näidise kirjelduse leiate peatükist *12. Projektikava kirjeldus*.

Olemasolevate investeeringupõhjenduste ja lähenemisviiside näited

Lähemalt tasub tutvuda näiteks järgmiste CSIRTi investeeringupõhjendustega.

- http://www.cert.org/csirts/AFI_case-study.html
  Finantsasutuse CSIRT asutamine: juhtumianalüüs

  Selles dokumendis jagatakse lugejatega õppetükke, mis saadi ühes finantsasutuses (dokumendis viidatakse sellele lühendiga „AFI“) turbeprobleeme käsitleva kava väljatöötamisel ja juurutamisel ning arvutiturbe juhtumitele reageerimise töörühma (CSIRT) asutamisel.

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  CERT POLSKA investeeringupõhjenduse kokkuvõte (PDF-vormingus slaidiseanss).

- http://www.auscert.org.au/render.html?it=2252
  Juhtumitele reageerimise töörühma (IRT) asutamine oli 1990. aastatel päris keeruline ettevõtmine. Paljudel IRTid asutavatel inimestel pole sellega mingeid varasemaid kogemusi. Selles dokumendis analüüsitakse rolli, mis IRTil võib ühiskonnas olla, ning käsitletakse probleeme, millele tuleks tähelepanu pöörata nii töörühma moodustamise ajal kui ka pärast tegevuse alustamist. Dokumendist võib kasu olla olemasolevatele IRTidele, kuna see võib aidata juhtida tähelepanu probleemidele, mida pole seni arutatud.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Infoturbe juhtumianalüüs, ettevõtte turvamine. Autor: Roger Benton

  See praktiline juhend kujutab endast ühe kindlustusfirma tervet ettevõtet hõlmavale turvasüsteemile ülemineku juhtumianalüüsi. Juhendi eesmärk on pakkuda välja tee, mida võiks turvasüsteemi loomisel või sellele üleminekul järgida. Alguses sai ettevõtte andmetele juurdepääsu kontrolli all hoida üksnes primitiivse elektroonilise turvasüsteemi abil. Riskid olid tõsised – väljaspool võrgukeskkonda puudusid igasugused tervikluskontrolli meetmed. Tootmisandmeid said lisada, muuta ja/või kustutada kõik elementaarsete programmeerimisoskustega inimesed.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Marriotti e-turbe strateegia: ettevõtluse ja IT koostöö

  Ettevõtte Marriott International, Inc. asepresidendi Chris Zoladzi hinnangul on e-äri turvamine pidev protsess, mitte ühekordne projekt. Just sellise arvamuse käis Zoladz välja hiljuti Intermedia Groupi toetusel Bostonis korraldatud e-turbe konverentsil ja messil. Marriotti teabekaitse asepresidendina käib kogu Zoladzi töö juriidilise osakonna kaudu, ehkki ta ise pole jurist. Tema ülesanne on kindlaks teha, kus hoitakse Marriotti kõige väärtuslikumat äriteavet ning kuidas seda ettevõtte sees ja ettevõttest välja liigutatakse. Turvalisust toetava tehnilise infrastruktuuri eest vastutab Marriottis eraldi IT-turbe arhitekt.

Fiktiivne CSIRT (toiming 7)

Äriplaani edendamine

Vastu on võetud otsus koguda seiku ja näitajaid ettevõtte senisest tegevusest. IT-turbe olukorrast statistilise ülevaate loomiseks on see äärmiselt kasulik. Statistika ajakohasena hoidmiseks tuleks teabe kogumist jätkata ka siis, kui CSIRT on juba loodud ja töötab.

Ühendust võeti muude riiklike CSIRTidega, kellega vahetati investeeringupõhjenduste koostamise osas kogemusi. CSIRTid olid nõu ja jõuga igati abiks, koostades slaide teabega IT-turbega seotud juhtumite viimase aja arengu ja juhtumitega kaasnevate kulude kohta.

Käesoleva dokumendi näidetes kasutatava fiktiivse CSIRTi puhul polnud vaja ettevõtte juhtkonda IT-äri olulisuses veenda ja seetõttu oli projekti alustamiseks loa saamine üsna lihtne. Ette valmistati investeeringupõhjendus ja projektikava (sh hinnang nii asutamisega kaasnevate kulude kui ka tegevuskulude kohta).

8 Tehniliste ja tööprotseduuride näited (töövood)

Seni oleme ära teinud järgmised toimingud.

1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda.
2. Millisele sektorile uus töörühm teenuseid osutab?
3. Mis liiki teenuseid võib CSIRT oma kliendibaasile osutada?
4. Keskkonna ja kliendibaasi analüüsimine.
5. Missiooni sõnastamine.
6. Äriplaani väljatöötamine.
   a. Finantsmudeli määratlemine.
   b. Organisatsioonilise struktuuri määratlemine.
   c. Töötajate palkamine.
   d. Kontori kasutuselevõtt ja varustamine.
   e. Infoturbepoliitika väljatöötamine.
   f. Koostööpartnerite otsimine.
7. Äriplaani edendamine.
   a. Investeeringupõhjendusele heakskiidu saamine.
   b. Kõige vajaliku kaasamine projektikavasse.

>> Järgmine toiming: CSIRTi sisseseadmine

Hästi määratletud töövoogude sisseseadmine aitab parendada töörühma töö kvaliteeti ja lühendada juhtumite või haavatavuste lahendamiseks vajaminevat aega.

Nagu näitekastides kirjeldatud, asub fiktiivne CSIRT osutama järgmisi CSIRTi põhiteenuseid:

- teated ja hoiatused;
- juhtumite käsitlemine;
- teadaanded.

Käesolevas peatükis tuuakse näiteid CSIRTi põhiteenuseid kirjeldavate töövoogude kohta. Samuti sisaldab see peatükk teavet selle kohta, kuidas mitmesugustest allikatest teavet koguda, selle asjakohasust ja ehtsust kontrollida ning seda kliendibaasile edasi anda. Peatüki viimases osas kirjeldatakse põhiprotseduure ja CSIRTi peamisi töövahendeid.

8.1 Klientide IT-süsteemi analüüsimine

Esmalt tuleks saada ülevaade sellest, millised IT-süsteemid on teie klientidel installitud. Nii saab CSIRT hinnata sissetuleva teabe asjakohasust ja teavet enne levitamist filtreerida, et kliendibaasi ei kallataks üle teabega, millest neil pole mingit kasu.

Alustada tasub lihtsalt, näiteks järgmist tüüpi Exceli töölehega:

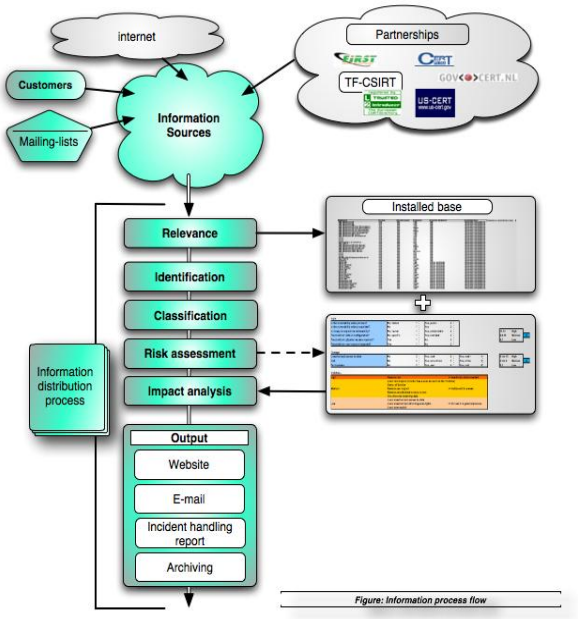
Kategooria	Rakendus	Tarkvara toode	Versioon	Süsteem	Süsteemi versioon	Klient
Lauaarvuti	Kontor	Excel	x-x-x	Microsoft	XP Pro	A
Lauaarvuti	Brauser	IE	x-x-	Microsoft	XP Pro	A
Võrk	Marsruuter	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Teenused	Veebiserver	Apache		Unix	x-x-x	B

Exceli filtreerimisfunktsiooni abil on lihtne valida õige tarkvara ja vaadata, millised kliendid mis liiki tarkvara kasutavad.

8.2 Teadete, hoiatuste ja teadaannete loomine

Teadete, hoiatuste ja teadaannete loomisel järgitakse sarnast töövoogu:

- teabe kogumine;
- teabe asjakohasuse ja allika hindamine;
- kogutud teabel põhinev riskianalüüs;
- teabe levitamine.



Joonis 9 : Teabeprotsessi voog

Järgmistes lõikudes kirjeldatakse seda töövoogu üksikasjalikumalt.

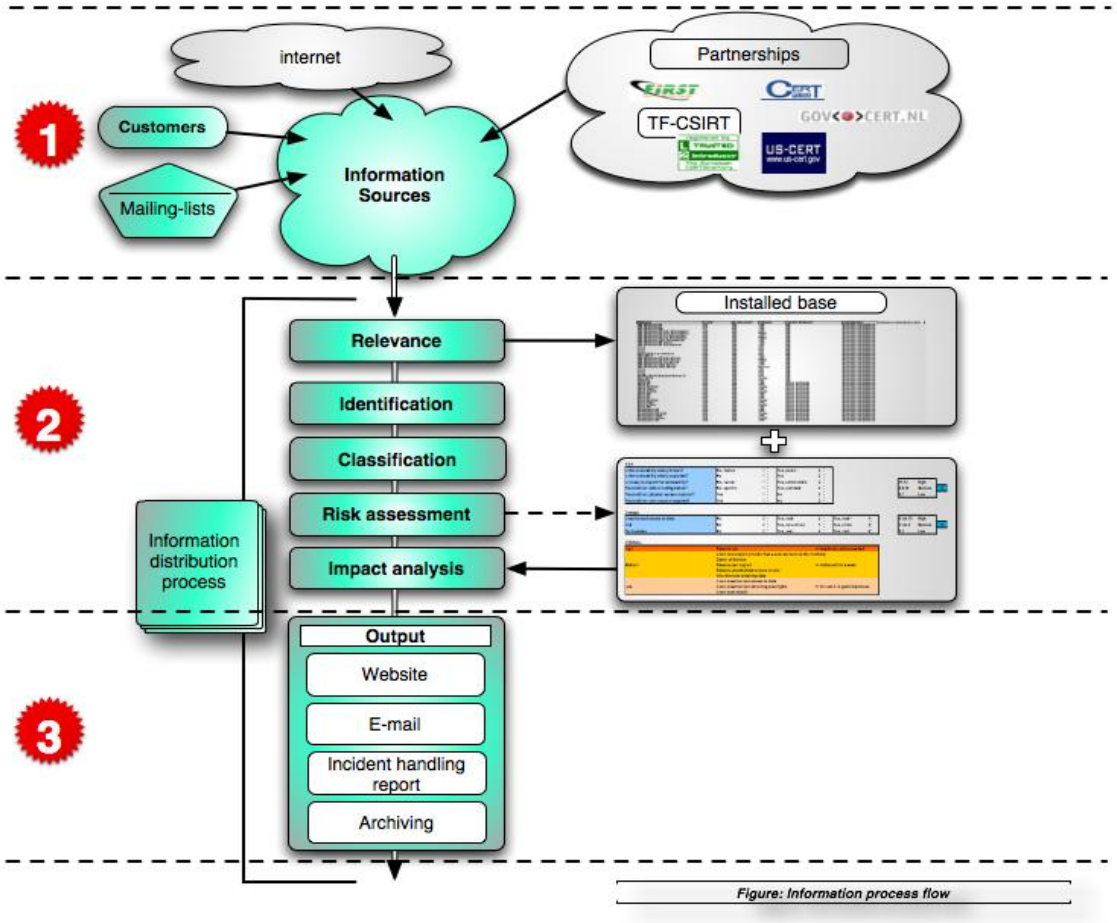


Figure: Information process flow

1. etapp: teabe kogumine haavatavuse kohta

Teenuste jaoks vajalikku teavet saab enamasti kahte tüüpi teabeallikatest:

- teave teie IT-süsteemide haavatavuse kohta;
- juhtumiaruanded.

Sõltuvalt ettevõtte ja IT-infrastruktuuri liigist on haavatavuse teabe allikaid (nii avalikke kui ka suletud allikaid) päris palju:

- avalikud ja suletud postitusloendid;
- tootjate teave toodete haavatavuse kohta;
- veebisaidid;
- Internetis leiduv teave (Google jms);
- avaliku ja erasektori partnerlused (FIRST, TF-CSIRT, CERT-CC, US-CERT jms), kes avaldavad teavet haavatavuse kohta.

Kõik need allikad suurendavad teadmisbaasi IT-süsteemi konkreetsetest haavatavustest.

Nagu eespool juba mainitud, on Internetis saadaval suurel hulgal kvaliteetseid ja hõlpsasti juurdepääsetavaid turbeteabeallikaid. 2006. aastal tegutsenud ENISA ajutine CERTi teenuste töörühm koostas ülevaatliku nimekirja, mis on kättesaadav alates 2006. aasta lõpust[19].

2. etapp: teabe hindamine ja riskianalüüs

Selle etapi käigus analüüsitakse konkreetse haavatavuse mõju kliendibaasi IT-infrastruktuurile.

Identifitseerimine
Saabuv teave haavatavuse tuleb alati identifitseerida selle allika järgi ning enne teabe edastamist kliendibaasile tuleb otsustada, kas allikas on piisavalt usaldusväärne. Nii hoitakse ära klientide äritegevuse põhjuseta häirimine, mis kahjustaks CSIRTi mainet.

[19] Ajutine CERTi teenuste töörühm: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Teate ehtsuse tuvastamise käiku kirjeldatakse järgmises näites.

Teate ja selle allika ehtsuse tuvastamise protseduur

Üldine kontrollnimekiri
1. Kas allikas on teada ja usaldusväärse allikana registreeritud?
2. Kas teave on edastatud tavapäraseid kanaleid kaudu?
3. Kas teade sisaldab „kummalist" teavet, mis „tundub" vale?
4. Järgige intuitsiooni – kui teave tundub kahtlane, siis ärge asuge kohe tegutsema, vaid veenduge esmalt teabe ehtsuses!

E-post – allikad
1. Kas saatja aadress on asutusele ja lähteloendile tuttav?
2. Kas PGP-allkiri on õige?
3. Kahtluse korral kontrollige sõnumi täielikke päiseid.
4. Kahtluse korral kontrollige saatja domeeni käskudega „nslookup" või „dig"[20].

Internet – allikad
1. Turvalise veebisaidiga (https://) ühenduse loomisel kontrollige brauseriserte.
2. Kontrollige allikat sisu ja (tehnilise) kehtivuse osas.
3. Kahtluse korral ärge klõpsake linke ega laadige alla tarkvara.
4. Kahtluse korral kontrollige domeeni käskudega „lookup" ja „dig" ning tehke „traceroute".

Telefon
1. Kuulake tähelepanelikult helistaja nime.
2. Kas helistaja hääl on teile tuttav?
3. Kahtluse korral küsige helistaja telefoninumbrit ja helistage talle tagasi.

Joonis 10 Teabe identifitseerimisprotseduuri näide

Asjakohasus
Varem koostatud ülevaadet installitud riistvarast ja tarkvarast saab kasutada sissetuleva haavatavuse teabe filtreerimiseks asjakohasuse alusel. Mõelda tasub järgmistele küsimustele: „Kas kliendid kasutavad seda tarkvaratoodet?" ja „Kas see teave on nende jaoks oluline?"

Klassifikatsioon
Osa vastuvõetud teabest võib olla salastatud või tähistatud piiratud kasutusõigusega teabena (nt teistelt töörühmadelt saadud juhtumiaruanded). Teabe töötlemisel tuleb alati lähtuda saatja nõudmistest ja töörühma või ettevõtte enda infoturbepoliitikast. Kasulik põhireegel on *„Ärge levitage teavet juhul, kui pole selge, et see on levitamiseks ette nähtud. Kahtluse korral küsige saatjalt levitamiseks luba."*

[20] CHIHTis identiteetide kontrollimiseks kasutatavad tööriistad:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Riski- ja mõjuanalüüs
Potentsiaalse või reaalse haavatavuse riski ja mõju määratlemiseks on mitu võimalust.

Risk määratletakse potentsiaalse võimalusena, et haavatavust võidakse ära kasutada. Oluliste teguritena tuleks arvestada näiteks järgmist.

- Kas haavatavus on hästi teada?
- Kas haavatavus on laialt levinud?
- Kas haavatavust on lihtne ära kasutada?
- Kas haavatavust saab ära kasutada kaugelt (võrgu kaudu)?

Neile küsimustele antud vastused annavad haavatavuse tõsidusest hea ülevaate.
Riski hindamisel võib kasu olla järgmisest lihtsast valemist:

Mõju = risk x potentsiaalne kahju

Potentsiaalsete kahjude näited:

- loata juurdepääs andmetele;
- teenuse blokeerimine (DOS);
- õiguste saamine või laiendamine.

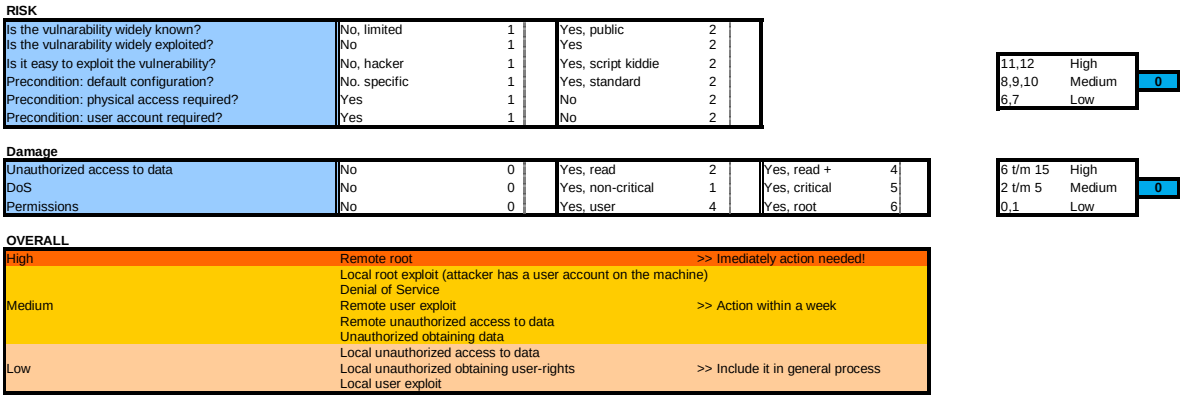
(Üksikasjalikumad liigitusskeemid leiate käesoleva peatüki lõpust.)

Pärast nendele küsimustele vastamist saab nõuandesse lisada üldhinnangu, mis teavitab kliente potentsiaalsest riskiastmest ja kahjudest. Sageli kasutatakse väga lihtsalt sõnastatud hinnangut – näiteks MADAL, KESKMINE ja KÕRGE.

Muud ulatuslikumad riskianalüüsiskeemid on järgmised:

GOVCERT.NL-i hindamisskeem[21]

Hollandi valitsussektori CSIRT GOVCERT.NL on riskianalüüsi jaoks välja töötanud maatriksi. Selle esialgne versioon koostati juba Govcert.nl'i algusjärgus ja seda värskendatakse pidevalt uuemate suundumustega.



Joonis 11 GOVCERT.NL-I hindamisskeem

Euroopa infoturbe edendamise kava ühtse nõuandevormingu kirjeldus[22]

Euroopa infoturbe edendamise kava (European Information Security Promotion Programme, EISPP) on projekt, mida kaasrahastab viienda raamprogrammi rakendamisel Euroopa Ühendus. EISPPi projekti eesmärk on töötada välja kogu Euroopat hõlmav raamistik mitte ainult turbealase teabe jagamiseks, vaid ka turbeteabe sisu määratlemiseks ning selle teabe väikestele ja keskmise suurusega ettevõtetele levitamise võimaluste leidmiseks. Andes Euroopa väikeste ja keskmise suurusega ettevõtete käsutusse vajalikud IT-turbe teenused, julgustatakse neid ettevõtteid senisest rohkem usaldama ja kasutama e-äri potentsiaali, mis omakorda toob kaasa rohkem uusi ärivõimalusi. EISPP aitab ellu viia Euroopa Ühenduse nägemust tervet Euroopa Liitu hõlmava oskusteabevõrgu loomisest.

DAF – Saksamaa nõuandevorming[23]

DAF on Saksamaa CERT-Verbundi algatus, mis moodustab ühe põhikomponendi turbenõuannete erinevate töörühmade poolt loomise ja vahetamise infrastruktuuris. DAF on välja töötatud eeskätt Saksamaa CERTide vajadusi silmas pidades. Standardi väljatöötamise ja haldamisega tegelevad CERT-Bund, DFN-CERT, PRESECURE ja Siemens-CERT.

[21] Haavatavuse maatriks: http://www.govcert.nl/download.html?f=33

[22] EISSP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

3. etapp: teabe levitamine

CSIRT saab valida ühe mitmest levitamisviisist, lähtudes kliendibaasi soovidest ja ettevõtte sidestrateegiast.

- Veebisait
- E-post
- Aruanded
- Arhiivimine ja uurimused

CSIRTi levitatavad turbenõuanded peaksid alati olema sarnase ülesehitusega. Nii on neid kergem lugeda ja lugeja leiab talle olulise teabe kiiresti üles.

Nõuanne peaks sisaldama vähemalt järgmist teavet.

Nõuande pealkiri
……

Viitenumber
……
Mõjutatud süsteemid
- ……
- ……

Seostuv süsteem + versioon
……
Risk (Kõrge-Keskmine-Madal)
……
Mõju / potentsiaalne kahju (Kõrge-Keskmine-Madal)
……
Välised ID-d: (CVE, haavatavuse bülletäänide ID-d)
……

Haavatavuse ülevaade
……

Mõju
……

Lahendus
……

Kirjeldus (üksikasjad)
……

Lisa
……

Joonis 12 Nõuande näidisskeem

Turbenõuande täieliku näite leiate peatükist *10. Harjutused*.

8.3 Juhtumite käsitlemine

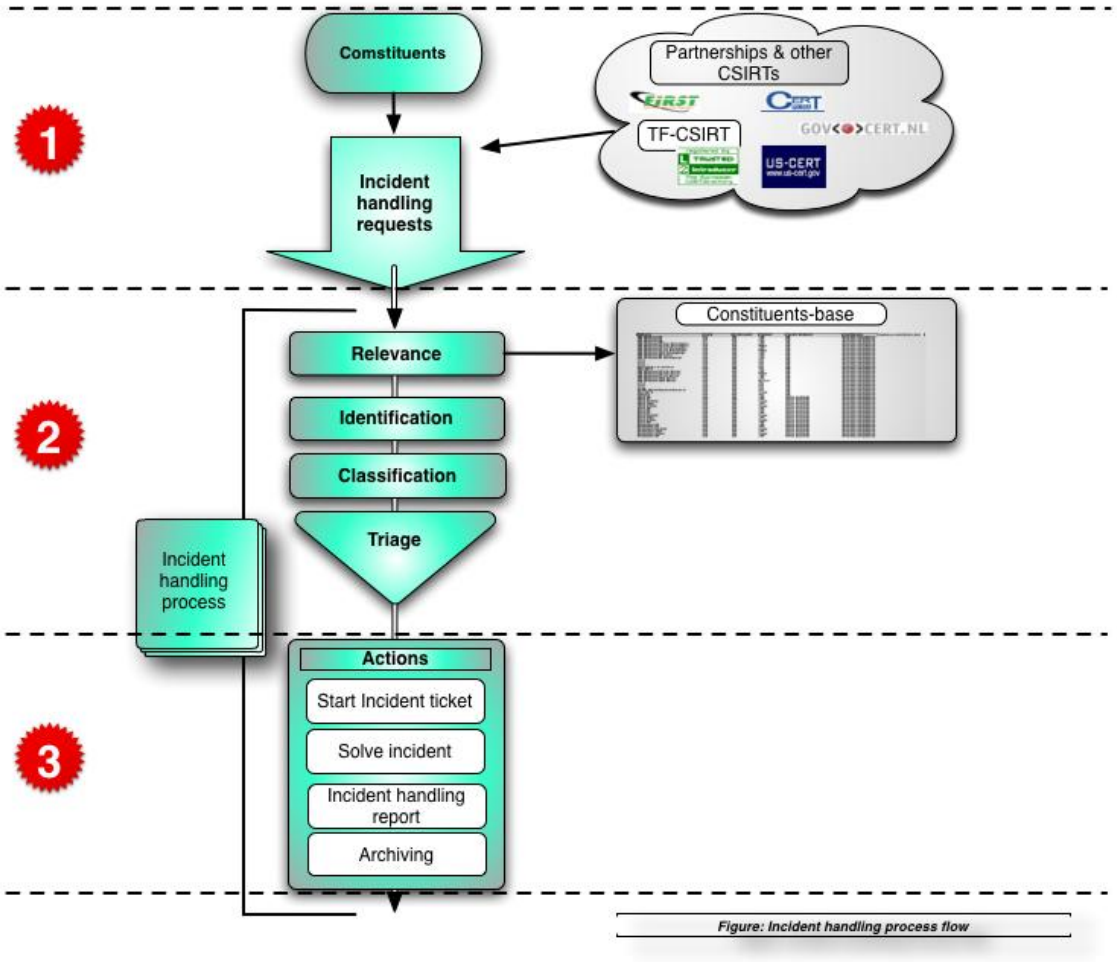
Nagu käesoleva peatüki sissejuhatuses mainitud, sarnaneb juhtumite käsitlemise käigus teabe töötlemise protsess teadete, hoiatuste ja teadaannete koostamisel kasutatava teabetöötlusprotsessiga. Teabe kogumine on aga enamasti erinev, kuna juhtumitega seotud andmeid kogutakse üldjuhul kliendibaasilt või teistelt töörühmadelt saadavate juhtumiaruannete kaudu või juhtumite käsitlemise ajal asjaosalistelt saadud tagasisidena. Teave liigub tavaliselt (krüptitud) e-posti kaudu, kuid vahel on vaja kasutada ka telefoni või faksi.

Teabe saamisel telefonitsi tasub alati kõik üksikasjad viivitamatult üles märkida, kas siis käsitsi või kasutades mõnda juhtumitöötluse või aruandluse tööriista. Kindlasti tuleb kohe (enne kõne lõpetamist) luua juhtumi viitenumber (kui juhtumil pole veel viitenumbrit) ja see juhtumist teatajale telefonitsi (või hiljem saadetavas meilisõnumis) teada anda, et edaspidi oleks sama juhtumit hõlpsam edasi arutada.

Käesoleva peatüki ülejäänud osas kirjeldatakse juhtumite käsitlemise põhitoiminguid. Juhtumihalduse ning kõigi seostuvate töövoogude ja alamtöövoogude väga põhjaliku analüüsi leiate CERT/CC dokumendist „*Defining Incident Management processes for CSIRTs*[24]“.

[24] Juhtumihaldusprotsesside määratlemine: http://www.cert.org/archive/pdf/04tr015.pdf

Juhtumite käsitlemine järgib enamasti järgmist töövoogu:



Joonis 13 Juhtumiprotsessi voog

1. etapp: juhtumiaruannete vastuvõtt

Nagu eespool mainitud, jõuavad juhtumiaruanded CSIRTi mitme kanali kaudu – enamasti e-postiga, kuid ka telefonitsi või faksiga.

Alati tasub kõik üksikasjad kohe juhtumiaruande vastuvõtmise käigus kindlaksmääratud kujul üles märkida. See tagab, et kriitilise tähtsusega teavet ei jäeta kogemata välja. Skeem võiks olla näiteks järgmine.

JUHTUMITEST TEATAMISE VORM

Palun täitke see vorm ja saatke faksi või meiliga järgmisel aadressil: ……..
Tärniga (*) tähistatud read on nõutavad.

Nimi ja organisatsioon
1. Nimi*:
2. Organisatsiooni nimi*:
3. Sektori tüüp:
4. Riik*:
5. Linn:
6. E-posti aadress*:
7. Telefoninumber*:
8. Muu:

Mõjutatud hostid
9. Hostide arv:
10. Hosti nimi ja IP*:
11. Hosti funktsioon*:
12. Ajavöönd:
13. Riistvara:
14. Operatsioonisüsteem:
15. Mõjutatud tarkvara:
16. Mõjutatud failid:
17. Turvalisus:
18. Hosti nimi ja IP:
19. Protokoll/port:

Juhtum
20. Viitenumber:
21. Juhtumi tüüp:
22. Juhtumi algus:
23. See on käimasolev juhtum: JAH EI
24. Avastamise aeg ja viis:
25. Teadaolevad haavatavused:
26. Kahtlased failid:
27. Vastumeetmed:
28. Üksikasjalik kirjeldus*:

Joonis 14 Juhtumiaruande kirjeldus

2. etapp: juhtumi hindamine

Selles etapis kontrollitakse teatatud juhtumi ehtsust ja olulisust ning juhtum liigitatakse.

Identifitseerimine

Tarbetute toimingute vältimiseks on hea mõte kontrollida, kas juhtumist teataja on usaldusväärne ning kas tegemist on teie või mõne teise CSIRTi kliendiga. Kehtivad peatükis *8.2 Teadete loomine* kirjeldatud reeglid.

Asjakohasus

Selles etapis peaksite kontrollima, kas juhtumitöötlustaotlus pärineb mõnelt CSIRTi kliendilt või kas teatatud juhtum on seotud klientide seas kasutusel olevate IT-süsteemidega. Kui tegemist pole kummagi eelmainitud variandiga, suunatakse aruanne enamasti ümber õigele CSIRTile[25].

Klassifikatsioon

Selles etapis valmistatakse ette sortimine, liigitades juhtumid nende tõsiduse järgi. Juhtumite liigitamine ehk klassifitseerimine jääb käesoleva dokumendi teemaulatusest välja. Alustuseks tasuks tutvuda CSIRTi juhtumite liigitamise skeemiga (näide ettevõtete CSIRTi jaoks):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Joonis 15 Juhtumite liigitamise skeem (allikas: FIRST)[26]

[25] CHIHTis identiteetide kontrollimiseks kasutatavad tööriistad:

http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] CSIRTi juhtumite liigitamine: http://www.first.org/resources/guides/csirt_case_classification.html

Sortimine

Sortimine (ingl. k. *triage*) on süsteem, mida meditsiinis või õnnetusjuhtumite korral kasutatakse piiratud meditsiiniressursside jaotamiseks juhul, kui hoolt vajavate haavatute arv ületab saadaolevate ressursside hulga, et abi saaks anda võimalikult paljudele patsientidele[27].

CERT/CC kirjeldab seda süsteemi järgmiselt.

Sortimine on äärmiselt oluline element igas juhtumihaldussüsteemis, kuid eriti juba töötavates CSIRTides. Sortimine aitab mõista, millest organisatsioonis teatatakse. See on funktsioon, mille kaudu kogu teave koondatakse ühte kontaktpunkti, et anda ülevaade terves ettevõttes toimuvatest tegevustest ja kõiki aruannetesse kaasatud andmeid omavahel põhjalikult võrrelda. Sortimisel antakse saabunud aruandele esialgne hinnang, seejärel pannakse aruanne edasise töötlemise ootamiseks järjekorda. Samuti võimaldab see alustada aruande või taotluse esialgset dokumenteerimist ja andmete sisestamist, kui seda pole juba tuvastamisprotsessi käigus tehtud.

Sortimisfunktsioon annab vahetu ülevaate kogu teatatud tegevuse hetkeseisust – millised aruanded on avatud või suletud, millised tegevused on ootel ning kui palju iga tüüpi aruandeid on vastu võetud. Selle protsessi abil saab tuvastada potentsiaalseid turbeprobleeme ja koormust jaotada vastavalt juhtumite tõsidusele. Sortimise käigus kogutud teavet saab kasutada ka haavatavus- ja juhtumisuundumuste analüüsimiseks ning juhtkonnale esitatava statistika loomiseks[28].

Sortimisega peaksid tegelema ainult kõige kogenumad töötajad, kuna see eeldab väga head arusaamist sellest, milline on juhtumite potentsiaalne mõju kliendibaasi konkreetsetele osadele, ja oskust otsustada, milline meeskonnaliige sobiks juhtumit töötlema kõige paremini.

[27] Sortimise kirjeldus Wikipedias: http://en.wikipedia.org/wiki/Triage

[28] Juhtumihaldusprotsesside määratlemine: http://www.cert.org/archive/pdf/04tr015.pdf

3. etapp: tegevused

Enamasti liiguvad sorditud juhtumid taotlusjärjekorda, mis on üks osa juhtumite käsitlemise tööriistast. Seda tööriista kasutab üks või mitu juhtumitöötlejat, kes tavaliselt toimivad järgmiselt.

Juhtumikirje loomine
Võimalik, et juhtumikirje number on eelmises etapis juba loodud (näiteks siis, kui juhtumist teatati telefonitsi). Kui see pole nii, tuleb luua number, mida kasutatakse kogu edaspidises selle juhtumiga seotud kirjavahetuses.

Juhtumi elutsükkel
Juhtumi käsitlemine pole tavaliselt otse lahenduseni viiv sirgjoon. Pigem tuleb samu etappe läbida korduvalt, kuni juhtum leiab lõpuks lahenduse ja kõigil asjaosalistel on kogu vajalik teave olemas. See ringikujuline lahenduskäik ehk juhtumi elutsükkel hõlmab järgmisi protsesse.

Analüüs:	Teatatud juhtumi kõigi üksikasjade analüüsimine.
Kontaktteabe hankimine:	Juhtumiga seotud aruandeteabe edastamiseks kõigile asjaosalistele (muudele CSIRTidele, rünnaku ohvritele ja arvatavasti ka rünnaku jaoks kasutatud süsteemide omanikele).
Tehnilise abi osutamine:	Rünnaku ohvrite aitamine, et juhtumi tagajärgedest toibumine kulgeks kiiresti, ning rünnaku kohta täiendava teabe kogumine.
Koordineerimine:	Teiste asjaosaliste (nt rünnaku jaoks kasutatud IT-süsteemi eest vastutava CSIRTi või teiste ohvrite) teavitamine.

Seda struktuuri nimetatakse elutsükliks, kuna üks samm viib järgmise sammuni ja viimane toiming (koordineerimine) võib omakorda kaasa tuua uue analüüsi, mille tulemusel algab tsükkel uuesti otsast peale. Protsess jõuab lõpule alles siis, kui kõik asjaosalised on kogu vajaliku teabe kätte saanud ja edasi andnud.

Juhtumi elutsükli üksikasjalikuma kirjelduse leiate CERT/CC CSIRTi käsiraamatust[29].

Juhtumitöötlusaruanne
Olge valmis vastama juhtkonna küsimustele ja koostage juba aegsasti juhtumite kohta aruanne. Samuti tasub omandatud kogemused ettevõttesiseseks kasutamiseks kirja panna, et töötajad saaksid tehtud vigadest õppust võtta ja neid edaspidiste juhtumite käsitlemisel vältida.

Arhiivimine
Tutvuge lähemalt arhiivimisreeglitega, mida on kirjeldatud peatükis *6.6 Infoturbepoliitika väljatöötamine*.

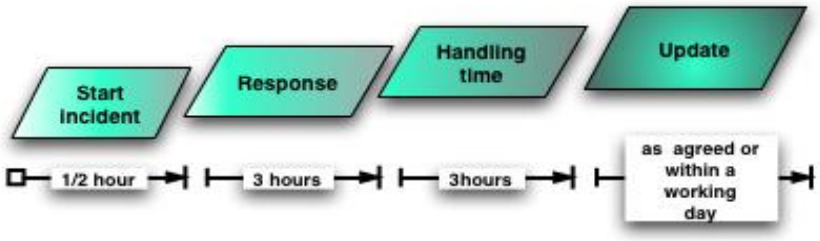
[29] CSIRTi käsiraamat: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Põhjalikumad juhendid juhtumihalduse ja juhtumi elutsükli kohta leiate lisa jaotisest *A.1 Lisateavet*.

8.4 Reageerimisajakava näide

Reageerimisajakava määratlemine on toiming, mida sageli eiratakse, kuid see peab kindlasti kuuluma igasse CSIRTi ja kliendibaasi vahel sõlmitud teenindustaseme lepingusse (SLA). Klientidele juhtumi käsitlemise ajal aktuaalse tagasiside andmine on väga oluline nii klientide kui ka töörühma maine jaoks.
Valede ootuste ärahoidmiseks tuleb reageerimisajad kliendibaasile kindlasti selgelt teatavaks teha. Järgmist väga lihtsustatud ajakava võib CSIRTi ja kliendibaasi vahel üksikasjalikuma teenindustaseme lepingu sõlmimisel kasutada lähtepunktina.

Selline on näiteks üks võimalik praktiline reageerimisgraafik, mis algab sissetulnud abitaotlusest:



Joonis 16 Reageerimisajakava näide

Samuti tasub kliendibaasi juhendada nende enda reageerimisaegade osas, rõhutades eriti seda, millal tuleks hädaolukorras CSIRTiga ühendust võtta. Kuna enamasti on mõistlik pöörduda CSIRTi poole kohe probleemi algusjärgus, tasub kliente julgustada kahtluse korral alati CSIRTiga ühendust võtma.

8.5 Saadaolevad CSIRTi tööriistad

Selles peatükis antakse põgus ülevaade tööriistadest, mida CSIRTid tavaliselt kasutavad. Siinkohal on ära toodud üksnes mõni näide. Lisateavet leiate artiklist „*Clearinghouse of Incident Handling Tools*“[30] (CHIHT).

E-posti ja sõnumite krüptimise tarkvara

- GNUPG http://www.gnupg.org/
  GnuPG on GNU projekti loodud terviklik tasuta juurutus OpenPGP standardist (RFC2440 definitsiooni järgi). GnuPG võimaldab andmeid ja kirjavahetust krüptida ning allkirjastada.

- PGP http://www.pgp.com/
  Kommertsversioon

Juhtumite käsitlemise tööriist

Tööriist, millega saab juhtumeid ja järeltegevust hallata ning tegevustel silma peal hoida.

- RTIR http://www.bestpractical.com/rtir/
  RTIR on avatud lähtekoodiga tasuta juhtumitöötlussüsteem, mille väljatöötamisel on lähtutud CERTi meeskondade ja muude juhtumireageerimistöörühmade vajadustest.

CRMi tööriistad

Kui teil on palju erinevaid kliente ning peate kohtumistel ja üksikasjadel hoolsalt silma peal hoidma, on abi CRMi (kliendisuhete halduse tarkvara) andmebaasist. Võimalikke variante on palju ja siin on toodud üksnes paar näidet:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforge (avatud lähtekoodiga tasuta versioon)
  http://www.sugarforge.org/

Teabe kontrollimine

- Website watcher http://www.aignes.com/index.htm
  See programm jälgib veebisaite uuenduste ja muudatuste osas.

- Watch that page http://www.watchthatpage.com/
  See teenus edastab veebisaitidel tehtud muudatuste teavet e-postiga (tasuta ja kommertsversioon).

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Kontaktteabe otsimine
Juhtumitest teatamiseks õige kontaktisiku leidmine pole lihtne ülesanne. Kasutada võib mõnda järgmistest teabeallikatest:

- RIPE[31]
- IRT-objekt[32]
- TI[33]

Lisaks on mõni kontaktteabe otsimise vahend ära toodud ka CHIHTi veebilehel[34].

Fiktiivne CSIRT (toiming 8)

Protsessivoogude ning tehniliste ja tööprotseduuride sisseseadmine
Fiktiivne CSIRT keskendub CSIRTi põhiteenuste osutamisele:

- teated ja hoiatused;
- teadaanded;
- juhtumite käsitlemine.

Töörühmas on välja töötatud hästi toimivad protseduurid, millest saavad hõlpsasti aru kõik töörühma liikmed. Samuti on fiktiivne CSIRT palganud õiguseksperdi, kes tegeleb vastutusega seotud küsimuste ja infoturbepoliitikaga. Töörühm on kasutusele võtnud mitu kasulikku tööriista ja saanud teiste CSIRTidega nõu pidades vajalikku teavet tööga seotud küsimuste kohta.

Loodud on ühtne mall turbenõuannete ja juhtumiaruannete jaoks. Juhtumite käsitlemiseks kasutab töörühm süsteemi RTIR (Request Tracker for Incident Response).

[31] RIPE whois: http://www.ripe.net/whois

[32] IRTi objekt RIPE andmebaasis: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] CHIHTis identiteetide kontrollimiseks kasutatavad tööriistad:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 CSIRTi koolitus

Seni oleme ära teinud järgmised toimingud.

1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda.
2. Millisele sektorile uus töörühm teenuseid osutab?
3. Mis liiki teenuseid võib CSIRT oma kliendibaasile osutada?
4. Keskkonna ja kliendibaasi analüüsimine.
5. Missiooni sõnastamine.
6. Äriplaani väljatöötamine.
   a. Finantsmudeli määratlemine.
   b. Organisatsioonilise struktuuri määratlemine.
   c. Töötajate palkamine.
   d. Kontori kasutuselevõtt ja varustamine.
   e. Infoturbepoliitika väljatöötamine.
   f. Koostööpartnerite otsimine.
7. Äriplaani edendamine.
   a. Investeeringupõhjendusele heakskiidu saamine.
   b. Kõige vajaliku kaasamine projektikavasse.
8. CSIRTi sisseseadmine.
   a. Töövoogude loomine
   b. CSIRTi tööriistade kasutuselevõtt

>> Järgmine toiming: töötajate koolitamine

Käesolevas peatükis on käsitletud kahte peamist CSIRTi koolituse allikat: TRANSITS ja CERT/CC kursuseid.

9.1 TRANSITS

TRANSITS on üle-Euroopaline projekt, mille eesmärk on arvutiturbe juhtumitele reageerimise töörühmade (CSIRTide) edendamine ja olemasolevate CSIRTide töö parendamine, tegeldes väljaõpetatud CSIRTi töötajate nappimise probleemi lahendamisega. Selleks on korraldatud kursusi, kus (uute) CSIRTide töötajaid koolitatakse CSIRTi teenuste osutamisega seotud organisatsiooniliste, tööalaste, tehniliste, turundusalaste ja õiguslike küsimuste osas.

Eelkõige on TRANSITS teinud järgmist:

- välja töötanud, värskendanud ja regulaarselt läbi vaadanud moodulipõhiste koolituskursuste materjale;
- korraldanud kursusematerjalide edastamiseks koolitusseminare;
- võimaldanud (uute) CSIRTide töötajate osalemist nendel koolitusseminaridel, pannes rõhku eelkõige ELi uute liikmesriikide töötajate osalemisele;
- levitanud koolituskursuste materjale ja taganud tulemuste kasutuselevõtu[35].

[35] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

ENISA aitab TRANSITSi kursuste korraldamisele kaasa ja toetab neid. Kui soovite kursustele registreerumise, nõuete ja hinna kohta täpsemat teavet, pöörduge ENISA CSIRTi spetsialistide poole:

CERT-Relations@enisa.europa.eu

Kursusematerjalide näidise leiate käesoleva dokumendi lisast.

9.2 CERT/CC

Arvuti- ja võrguinfrastruktuuride keerukus ja nende administreerimisega seotud probleemid teevad võrguturbe õige haldamise üsna raskeks. Võrgu- ja süsteemiadministraatoritel pole süsteemi rünnakute eest kaitsmiseks ja kahjude minimeerimiseks tavaliselt ei piisavalt töötajaid ega sisseseatud turbepoliitikaid. Seetõttu on arvutiturbega seotud juhtumite arv aina kasvamas.
Arvutiturbejuhtumite ilmnemisel peavad asutused neile reageerima kiiresti ja tõhusalt. Mida kiiremini asutus juhtumi avastab, seda analüüsib ja sellele reageerib, seda paremini saab kahjusid piirata ja taastekulusid all hoida. Arvutiturbe juhtumitele reageerimise töörühma (CSIRT) loomine annab asutuse käsutusse nii kiire reageerimisvõime kui ka võimaluse edaspidiseid juhtumeid ära hoida.

CERT-CC pakutavad kursused on mõeldud nii juhtkonnale kui ka tehnikutele. Koolitused hõlmavad näiteks arvutiturbe juhtumitele reageerimise töörühmade (CSIRTide) asutamist ja juhtimist, turbejuhtumitele reageerimist ja nende analüüsimist ning võrguturbe täiustamist. Kui pole märgitud teisiti, korraldatakse kursused Ameerika Ühendriikides Pennsylvania osariigis Pittsburghis. Lisaks koolitavad CERT-CC töötajad arvutiturbe alal ka Carnegie Melloni ülikooli õppureid.

CSIRTidele suunatud saadaolevad CERT/CC kursused[36]

Arvutiturbe juhtumitele reageerimise töörühma (CSIRTi) asutamine
Arvutiturbe juhtumitele reageerimise töörühmade (CSIRTide) juhtimine
Juhtumitöötluse põhitõed
Üksikasjalik juhtumikäsitlus tehnilisele personalile

Kursusematerjalide näidise leiate käesoleva dokumendi lisast.

Fiktiivne CSIRT (toiming 9)
Töötajate koolitamine Fiktiivne CSIRT otsustab saata kõik tehnilised töötajad järgmistele pakutavatele TRANSITSi kursustele. Meeskonnajuht osaleb lisaks ka CERT/CC kursusel *CSIRTi juhtimine*.

[36] CERT/CC kursused: http://www.sei.cmu.edu/products/courses

10 Harjutus: nõuande koostamine

Seni oleme ära teinud järgmised toimingud.

1. Arusaam CSIRTi olemusest ja sellest, milliseid eeliseid see võib pakkuda.
2. Millisele sektorile uus töörühm teenuseid osutab?
3. Mis liiki teenuseid võib CSIRT oma kliendibaasile osutada?
4. Keskkonna ja kliendibaasi analüüsimine.
5. Missiooni sõnastamine.
6. Äriplaani väljatöötamine.
   a. Finantsmudeli määratlemine.
   b. Organisatsioonilise struktuuri määratlemine.
   c. Töötajate palkamine.
   d. Kontori kasutuselevõtt ja varustamine.
   e. Infoturbepoliitika väljatöötamine.
   f. Koostööpartnerite otsimine.
7. Äriplaani edendamine.
   a. Investeeringupõhjendusele heakskiidu saamine.
   b. Kõige vajaliku kaasamine projektikavasse.
8. CSIRTi sisseseadmine.
   a. Töövoogude loomine
   b. CSIRTi tööriistade kasutuselevõtt
9. Töötajate koolitamine

>> Järgmiseks tuleb läbi teha paar harjutust ja oletegi päris töö jaoks valmis!

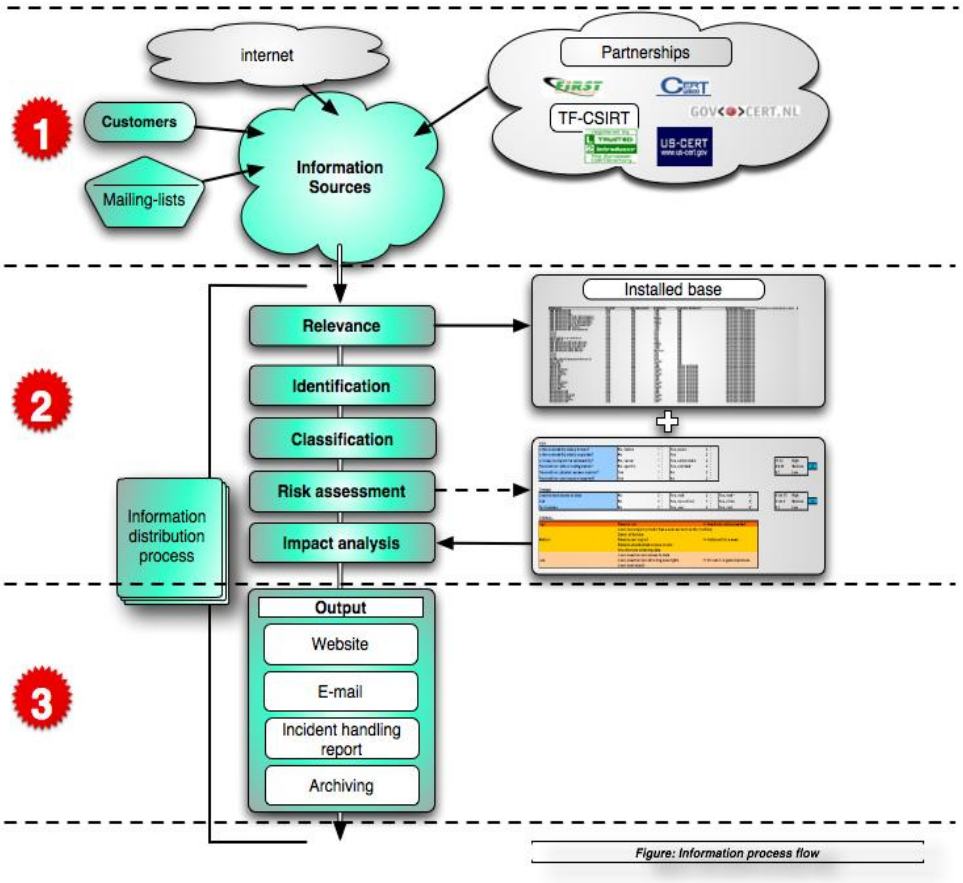
Tegevuse illustreerimiseks kirjeldatakse käesolevas peatükis ühe igapäevase CSIRTi toimingu ehk turbenõuande loomise näidisharjutust.

Turbenõuande koostamise vajaduse põhjustas järgmine Microsofti turbenõuanne.

Bülletääni ID	**Microsofti turbebülletään MS06-042**
Bülletääni tiitel	**Internet Exploreri koondturvavärskendus (918899)**
Kommenteeritud kokkuvõte	Käesolev värskendus lahendab Internet Exploreris mitu haavatavust, mis võivad lubada koodi kaugkäivitamist.
Maksimaalne raskusaste	Kriitiline
Haavatavuse mõju	Koodi kaugkäivitamine
Mõjutatud tarkvara	**Windows, Internet Explorer.** Lisateavet leiate jaotisest „Mõjutatud tarkvara ja allalaadimiskohad“.

Selles tootja väljaantud bülletäänis käsitletakse Internet Exploreris hiljuti leitud haavatavust. Tootja avaldab selle tarkvara jaoks mitu Microsoft Windowsi eri versioone hõlmavat parandust.

Pärast seda, kui fiktiivne CSIRT on selle haavatavuse teabe postitusloendi kaudu vastu võtnud, alustab CSIRT peatükis *8.2 Teadete, hoiatuste ja teadaannete loomine*



käsitletud töövoogu.

1. etapp: haavatavuse teabe kogumine

Esmalt tuleks sirvida tootja veebisaiti. Nii saab fiktiivne CSIRT veenduda teabe ehtsuses ning koguda haavatavuse ja sellest mõjutatud IT-süsteemide kohta üksikasjalikumat teavet.

2. etapp: teabe hindamine ja riskianalüüs

Identifitseerimine
Teave on juba kontrollitud: võrreldi e-postiga saadud haavatavuse teavet tootja veebisaidil leiduva tekstiga.

Asjakohasus
Fiktiivne CSIRT võrdleb veebisaidil avaldatud mõjutatud süsteemide loetelu kliendibaasis kasutusel olevate süsteemide loendiga. Kuna selgub, et vähemalt üks klient kasutab Internet Explorerit, on haavatavuse teave tõepoolest asjakohane.

Kategooria	Rakendus	Tarkvara-toode	Versioon	OS	OS-i versioon	Klient
Lauaarvutid	Brauser	IE	x-x-	Microsoft	XP Pro	A

Klassifikatsioon
Kuna teave on avalik, tohib seda kasutada ja edasi levitada.

Riski- ja mõjuanalüüs
Järgmistele küsimustele vastamisel selgub, et riski- ja mõjuaste on *kõrge* (Microsofti hinnangul *kriitiline*).

RISK

Kas haavatavus on hästi teada?	J
Kas haavatavus on laialt levinud?	J
Kas haavatavust on lihtne ära kasutada?	J
Kas haavatavust saab ära kasutada kaugelt (võrgu kaudu)?	J

KAHJUD
Haavatavuse tõttu on võimalik kaugjuurdepääs ja potentsiaalselt ka koodi kaugkäivitamine. Kuna see haavatavus hõlmab mitut probleemi, on kahjude riskiaste *kõrge*.

3. etapp: levitamine

Fiktiivne CSIRT on asutusesisene CSIRT. Sidekanalitena on saadaval e-post, telefon ja sisevõrgusait. CSIRT koostab järgmise nõuande, võttes aluseks peatükis *8.2 Teadete, hoiatuste ja teadaannete loomine* käsitletud malli.

Nõuande pealkiri
Internet Exploreris on leitud mitu haavatavust

Viitenumber
082006-1

Mõjutatud süsteemid
- Kõik Microsofti tarkvara kasutavad lauaarvutid

Seostuv süsteem + versioon
- Microsoft Windows 2000 koos hoolduspaketiga Service Pack 4
- Microsoft Windows XP koos hoolduspaketiga Service Pack 1 ja Microsoft Windows XP koos hoolduspaketiga Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 ja Microsoft Windows Server 2003 koos hoolduspaketiga Service Pack 1
- Microsoft Windows Server 2003 Itaniumi-põhiste arvutisüsteemide jaoks ja Microsoft Windows Server 2003 koos hoolduspaketiga SP1 Itaniumi-põhiste arvutisüsteemide jaoks
- Microsoft Windows Server 2003 x64 Edition

Risk (Kõrge-Keskmine-Madal)
KÕRGE

Mõju / potentsiaalne kahju (Kõrge-Keskmine-Madal)
KÕRGE

Välised ID-d: (CVE, haavatavuse bülletäänide ID-d)
MS-06-42

Haavatavuse ülevaade
Microsoft on Internet Explorerist leidnud mitu kriitilise tähtsusega haavatavust, mis võivad lubada koodi kaugkäivitamist.

Mõju
Ründaja võib saada täieliku kontrolli teie süsteemi üle: installida programme, lisada kasutajaid ning vaadata, muuta või kustutada teie andmeid. Leevendava tegurina võib kõik eeltoodu aset leida üksnes juhul, kui kasutaja on arvutisse sisse logitud administraatori õigustes. Piiratud õigustega kasutajate korral ei pruugi see mõju olla nii ulatuslik.

Lahendus
Installige Internet Exploreri turvapaik viivitamatult

Kirjeldus (üksikasjad)
Lisateavet leiate siit: ms06-042.mspx

Lisa
Lisateavet leiate siit: ms06-042.mspx

Nõuanne on nüüd levitamiseks valmis. Kuna tegemist on kriitilise tähtsusega bülletääniga, on soovitatav klientidele võimalusel ka helistada.

Fiktiivne CSIRT (toiming 10)

Harjutused

Paari esimese töönädala jooksul kasutas fiktiivne CSIRT harjutamiseks mitut fiktiivset juhtumit (need saadi näidetena teistelt CSIRTidelt). Lisaks anti välja mitu turbenõuannet, mis põhinesid riist- ja tarkvaratootjatelt saadud tegelikul haavatavuse teabel. CSIRTi töötajad kohandasid selle teabe oma kliendibaasi vajadustele vastavaks.

11 Lõppsõna

Sellega saabki juhend läbi. Käesoleva dokumendi otstarve on CSIRTi asutamiseks vajalikest protsessidest üksnes väga põgusa ülevaate andmine. Juhend ei pretendeeri täielikkusele ega lasku väga konkreetsetesse üksikasjadesse. Lisalugemiseks kasuliku kirjanduse ülevaate leiate jaotisest *A.1 Lisateavet*.

Fiktiivne CSIRT peaks nüüd ette võtma järgmised olulised toimingud:

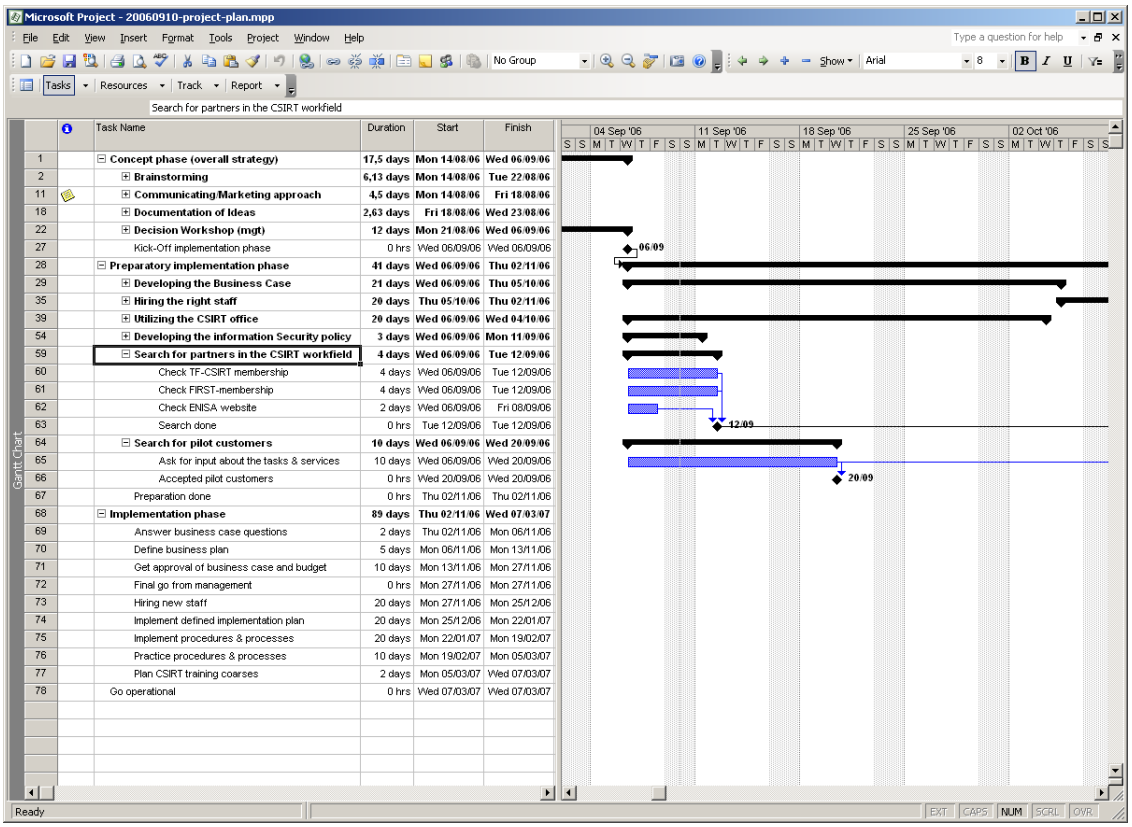
- klientidelt tagasiside saamine osutatavate teenuste täpsemaks kohandamiseks;
- igapäevase töörutiini sisseseadmine;
- hädaolukordade jaoks harjutamine;
- erinevate CSIRTi kogukondadega suhtlemine, et tulevikus saaks nende vabatahtlikku töösse ka oma panuse anda.

12 Projektikava kirjeldus

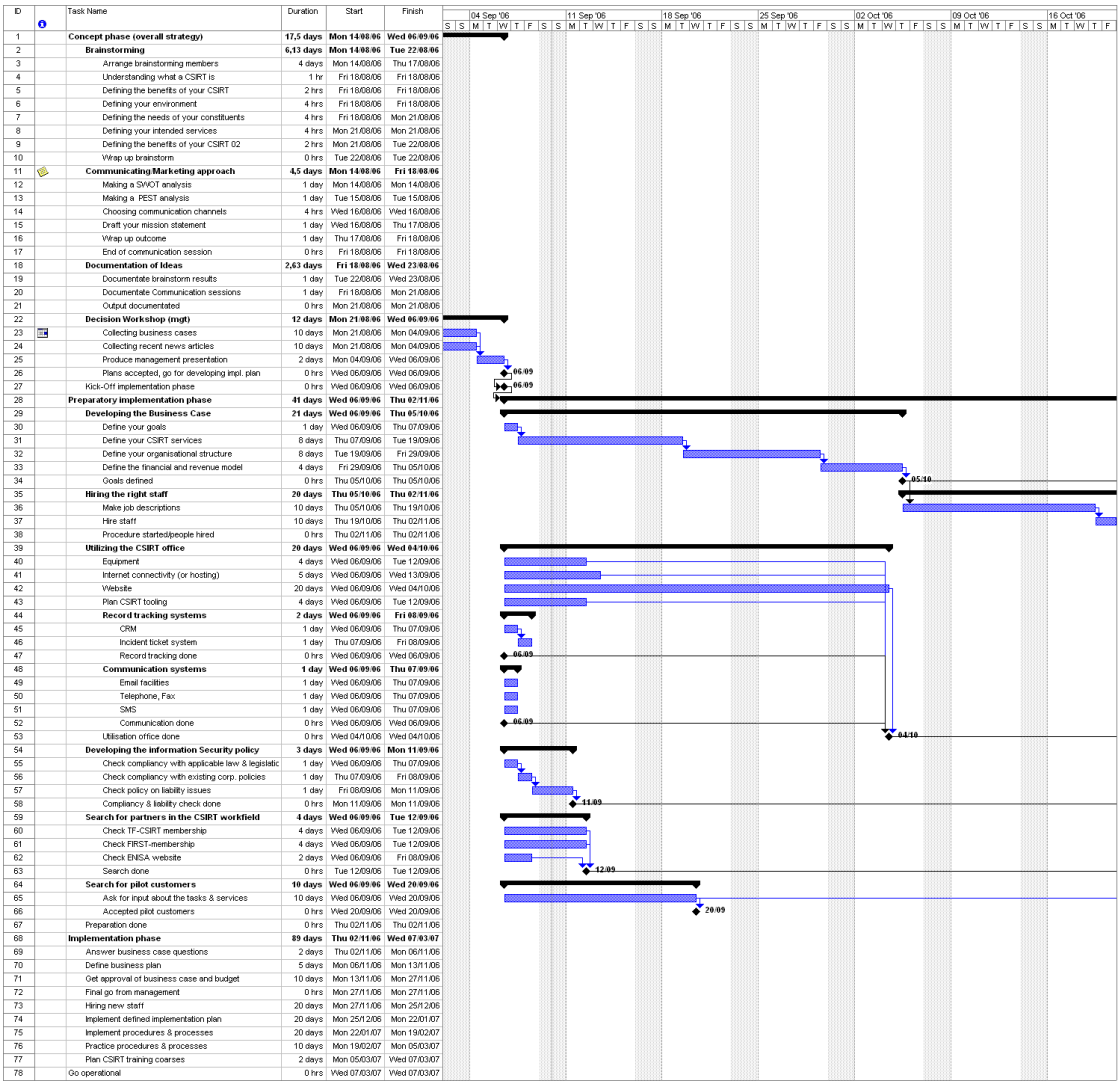
MÄRKUS. Projektikava on esialgne hinnang vajamineva aja kohta. Sõltuvalt sellest, millised ressursid on saadaval, võib projekti tegelik kestus kavast erineda.

Projektikava on mitmes vormingus saadaval nii CD-l kui ka ENISA veebisaidil. See hõlmab täielikult kõiki käesolevas dokumendis kirjeldatud protsesse.

Kuna projektikava põhiversioon on ära toodud Microsoft Projecti vormingus, saab seda mugavalt kasutada otse selles projektihaldustööriistas.



Joonis 17 Projektikava



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**41 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilisation office done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Joonis 18 Projektikava koos kõigi toimingute ja Gantti diagrammi osaga

Projektikava on saadaval ka CVS- ja XML-vormingus. Lisateavet saate küsida ENISA CSIRTi spetsialistidelt: CERT-Relations@enisa.europa.eu.

LISA

A.1 Lisateavet

CSIRTide käsiraamat (CERT/CC)
Väga laiahaardeline teatmeteos, milles käsitletakse kõiki CSIRTi töö jaoks olulisi teemasid
Allikas: http://www.cert.org/archive/pdf/csirt-handbook.pdf

CSIRTide juhtumihaldusprotsesside määratlemine: pidevalt täiendatav
Juhtumihalduse põhjalik analüüs
Allikas: http://www.cert.org/archive/pdf/04tr015.pdf

Arvutiturbe juhtumitele reageerimise töörühmade (CSIRTide) tegevuse olek
Põhjalik analüüs tegelikust olukorrast, mis käsitleb CSIRTide hetkeseisu kogu maailmas, hõlmates muu hulgas ka ajalugu ja statistikat
Allikas: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Põhjalik kirjeldus selle kohta, milliseid õppetükke andsid GOVCERT.NL-i ja Hollandi riikliku teavitusteenuse De Waarschuwingsdienst asutamine
Allikas: http://www.govcert.nl/render.html?it=69

RFC 2350: ootused arvutiturbe juhtumitele reageerimisele
Allikas: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] arvutiturbe juhtumite käsitlemise juhend
Allikas: http://www.securityunit.com/publications/sp800-61.pdf

ENISA ülevaade CERTi tegevusest Euroopas
Teatmeteos, mis sisaldab teavet Euroopas töötavate CSIRTide ja nende tegevuse kohta
Allikas: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: National Institute of Standards and Technologies

A.2 CSIRTi teenused

Selle loendi eest tuleb tänu avaldada CERT/CC-le

Reaktiivsed teenused	***Proaktiivsed teenused***	***Artefaktide käsitlemine***
• Teated ja hoiatused • Juhtumitöötlus • Juhtumianalüüs • Kohapealne reageerimine juhtumitele • Juhtumitele reageerimise tugiteenused • Juhtumitele reageerimise koordineerimine • Haavatavuste käsitlemine • Haavatavuste analüüs • Haavatavustele reageerimine • Haavatavustele reageerimise koordineerimine	• Teadaanded • Tehnoloogiaseire • Turbeauditid või -hindamised • Turvalisuse konfigureerimine ja haldamine • Turbetööriistade väljatöötamine • Sissetungituvastusteenused • Turbealase teabe levitamine	• Artefaktianalüüs • Artefaktidele reageerimine • Artefaktidele reageerimise koordineerimine
		Turbekvaliteedi juhtimine
		• Riskianalüüs • Majandustegevuse jätkamine ja tõrgete kõrvaldamine • Turbealane nõustamine • Teadlikkuse suurendamine • Haridus/koolitus • Tootehindamine või -sertifitseerimine

Joonis 19 CSIRTi teenuste loend, CERT/CC

Teenuste kirjeldused

Reaktiivsed teenused

Reaktiivsete teenuste eesmärk on kiire reageerimine abipalvetele, CSIRTi klientidelt saadud juhtumiteadetele ning kõigile CSIRTi süsteemide vastu suunatud ohtudele või rünnakutele. Mõne teenuse osutamise võib algatada kolmandalt osapoolelt saadud teatis või seire- või IDS-logide ja teatiste jälgimine.

Teated ja hoiatused

See teenus hõlmab rünnakut, turvahaavatavust, sissetungihoiatust, arvutiviirust või pettust kirjeldava teabe levitamist ning lühiajalise tegevuskava väljapakkumist selliste ohtudega kaasnevate probleemide lahendamiseks. Teade, hoiatus või nõuanne saadetakse vastusena tegelikult esinevale probleemile, teavitamaks kliente vastavast tegevusest ja andmaks nõu, kuidas arvutisüsteemi kaitsta või juba kahjustatud süsteemi taastada. CSIRT võib teabe ise koostada, kuid lisaks sellele võidakse levitada ka tootjatelt, teistelt CSIRTidelt või turbespetsialistidelt või klientidelt saadud teavet.

Juhtumikäsitlemine

Juhtumikäsitlemine hõlmab taotluste ja teadete vastuvõttu, sortimist ja neile reageerimist ning juhtumite ja sündmuste analüüsimist. Reageerimine võib hõlmata näiteks järgmisi tegevusi:

- selliste süsteemide ja võrkude kaitsmine, mida on juba rünnatud või mida sissetungijad võivad ohustada;
- lahenduste ja leevendusstrateegiate pakkumine vastavate nõuannete või teadete kaudu;
- rünnakule viitava tegevuse otsimine võrgu muudest osadest;
- võrguliikluse filtreerimine;
- süsteemide taastamine;
- süsteemide paikamine või parandamine;
- muude reageerimis- või lahendusstrateegiate väljatöötamine.

Kuna erinevat tüüpi CSIRTides on juhtumite käsitlemine lahendatud erinevalt, saab seda teenust täpsemalt liigitada sooritatud tegevuste ja osutatud abi tüübi alusel.

Juhtumianalüüs

Juhtumianalüüsil on palju tasemeid ja ohtralt alamteenuseid. Sisuliselt tähendab juhtumianalüüs kogu mõne kindla juhtumi või sündmusega seotud saadaoleva teabe ja täiendava tõendusmaterjali või artefaktide uurimist. Analüüsi eesmärk on juhtumi leviku, juhtumi põhjustatud kahjude ulatuse, juhtumi olemuse ning võimalike reageerimisstrateegiate või lahenduste väljaselgitamine. CSIRT võib haavatavuse ja artefaktide analüüsi (vt allpool) tulemusi kasutada kindla süsteemi puhul aset leidnud tegevustest kõige täielikuma ja ajakohasema analüüsi koostamiseks. CSIRT võrdleb juhtumitega seotud tegevusi üksteisega, et teha kindlaks kõik võimalikud juhtumitevahelised seosed, suundumused, mustrid või sissetungija signatuurid. Juhtumianalüüsi raames võidakse osutada kahte alamteenust, kuid see sõltub CSIRTi missioonist, eesmärkidest ja tööprotsessidest.

Asitõendite kogumine

Rünnatud arvutisüsteemis leiduvate asitõendite kogumine, säilitamine, dokumenteerimine ja analüüsimine, et teha kindlaks süsteemis aset leidnud muudatused ja aidata kaasa sissetungile eelnenud sündmuste rekonstrueerimisele. Teabe ja asitõendite kogumine tuleb kindlasti dokumenteerida nii, et kogu protsess oleks tõestatav ja kogutud teavet saaks asitõenditena kasutada ka kohtus. Asitõendite kogumine hõlmab muu hulgas näiteks mõjutatud süsteemi kõvakettast bititõmmisekoopia tegemist, süsteemist muudatuste (nt uute programmide, failide, teenuste ja kasutajate) otsimist, töötavate protsesside ja avatud portide vaatamist ning nn Trooja hobuste ja tööriistakomplektide otsimist. Seda tööd tegevad CSIRTi töötajad peaksid olema valmis selleks, et neid võidakse eksperdina kohtusse tunnistajaks kutsuda.

Jälgimine või jälitamine

Sissetungija lähtekoha leidmine või nende süsteemide tuvastamine, millele sissetungijal oli juurdepääs. See tegevus võib hõlmata uurimist (jälgimist ehk jälitamist), kuidas sissetungija mõjutatud süsteemi ja seostuvatesse süsteemidesse sisenes, milliseid süsteeme juurdepääsu saamiseks kasutati, kust rünnak alguse sai ning milliseid muid süsteeme ja võrke on rünnaku raames kasutatud. Samuti võib see hõlmata sissetungija

isiku tuvastamise katset. CSIRT võib seda teha üksi, kuid enamasti tehakse seda koostöös politsei, Interneti-teenuse pakkujate või muude asjaga seotud asutustega.

Kohapealne reageerimine juhtumitele

CSIRT osutab klientidele juhtumist taastumiseks otsest kohapealset abi. CSIRT analüüsib mõjutatud süsteeme füüsiliselt ning parandab või taastab süsteemid, mitte ei piirdu üksnes telefonitsi või e-posti kaudu juhtumile reageerimise tugiteenuste osutamisega (vt allpool). See teenus hõlmab kõiki kohapealseid tegevusi, mis on arvatava või tegelikult esinenud juhtumi lahendamiseks nõutavad. Kui CSIRT ei asu mõjutatud süsteemiga samas kohas, peavad töörühma liikmed selle teenuse osutamiseks ja juhtumile reageerimiseks kohale sõitma. Kohalik töörühm võib aga juba kohapeal töötada, osutades juhtumile reageerimise teenust oma igapäevatöö raames. See võib juhtuda näiteks siis, kui juhtumitöötlus on CSIRTi asemel tegutsevate süsteemi- võrgu- või turbeadministraatorite töö tavaline osa.

Juhtumitele reageerimise tugiteenused

CSIRT abistab ja juhendab rünnaku ohvreid juhtumist taastumisel telefonitsi või e-posti, faksi või asjakohase dokumentatsiooni kaudu. Muu hulgas võidakse pakkuda tehnilist abi kogutud andmete tõlgendamisel, anda kontaktteavet või juhendada klienti leevendus- ja taastestrateegiate osas. Erinevalt eespool kirjeldatust ei hõlma see teenus otsest kohapealset reageerimist juhtumile. Selle asemel juhendab CSIRT klienti kaugelt, et klientasutuse töötajad saaksid taastamistoimingud ise läbi viia.

Juhtumitele reageerimise koordineerimine

CSIRT koordineerib juhtumisse kaasatud osapoolte reaktsioone juhtumile. Enamasti hõlmab see rünnaku ohvrit, muid rünnakuga seotud osapooli ja teisi, kes vajavad rünnaku analüüsimisel abi. Samuti võib see hõlmata ohvrile IT-tugiteenuseid osutavaid asutusi (nt Interneti-teenuse pakkujat, muid CSIRTe) ning kohapealseid süsteemi- ja võrguadministraatoreid. Koordineerimistöö võib sisaldada kontaktteabe kogumist, osapoolte teavitamist nende võimalikust seotusest rünnakuga (rünnaku ohvri või allikana), rünnakuga seotud osapoolte arvu kohta statistika kogumist ning teabevahetuse ja analüüsi hõlbustamist. Osa koordineerimistööst võib hõlmata asutuse juristi, personali- või avalike suhete osakonna teavitamist ja koostööd nende osakondadega. Samuti võib see hõlmata koostööd politseiga. See teenus ei hõlma otsest kohapealset reageerimist juhtumile.

Haavatavuste käsitlemine

Haavatavuste käsitlemine hõlmab riistvara- ja tarkvarahaavatavustega seotud teabe ja teadete vastuvõttu, haavatavuste olemuse, töömehhanismide ja mõjude analüüsimist ning haavatavuste tuvastamise ja parandamise jaoks reageerimisstrateegiate väljatöötamist. Kuna erinevat tüüpi CSIRTides on haavatavuste käsitlemine lahendatud erinevalt, saab seda teenust täpsemalt liigitada sooritatud tegevuste ja osutatud abi tüübi alusel.

Haavatavuste analüüs

CSIRT analüüsib ja uurib riistvaras või tarkvaras leitud haavatavusi. Analüüsimine hõlmab arvatavate haavatavuste kinnitamist ja riistvara- või tarkvarahaavatavuse tehnilist ülevaatust, et teha kindlaks haavatavuse asukoht ja selle võimaliku kuritarvitamise viisid. Analüüsimine võib sisaldada lähtekoodi läbivaatamist, haavatavuse

asukoha siluri abil kindlaksmääramist ning probleemi testsüsteemis esilekutsumise katset.

Haavatavustele reageerimine

See teenus hõlmab haavatavuse leevendamiseks või parandamiseks sobiva vastuse väljaselgitamist. See protsess võib sisaldada paikade, veaparanduste ja lahenduste väljatöötamist või uurimist. Samuti hõlmab see teiste asjaosaliste teavitamist leevendusstrateegiast (nt nõuannete või teadete koostamise ja levitamise kaudu). Teenus võib hõlmata ka otsest reageerimist – paikade, veaparanduste või lahenduste installimist.

Haavatavustele reageerimise koordineerimine

CSIRT teavitab ettevõtet või kliendibaasi haavatavusest ning jagab teavet haavatavuse parandamise või leevendamise kohta. CSIRT kontrollib, kas haavatavusele reageerimise strateegia on edukalt kasutusele võetud. See teenus võib hõlmata suhtlemist tootjate, teiste CSIRTide, tehnikaspetsialistide, klientide ning haavatavuse algselt avastanud või sellest teatanud isikute või rühmadega. Ettevõetavate tegevuste seas on haavatavuse analüüsi või haavatavuse teate koostamise hõlbustamine, vastavate dokumentide, paikade või lahenduste avaldamiskava kooskõlastamine ning erinevate osapoolte poolt tehtud tehnilise analüüsi sünteesimine. Samuti võib see teenus hõlmata haavatavuse teabe ja sellele vastavate reageerimisstrateegiate avaliku või eraarhiivi või teabebaasi haldamist.

Artefaktide käsitlemine

Artefakt on süsteemist leitud fail või objekt, mis võib olla seotud süsteemide ja võrkude sondeerimise või ründamisega või mida kasutatakse turbemeetmete nurjamiseks. Artefaktid võivad olla näiteks arvutiviirused, nn Trooja hobused, ussviirused, kuritarvitamist võimaldavad skriptid ja tööriistakomplektid.
Artefaktide käsitlemine hõlmab rünnakutes, luurel ja muude volitamata või süsteemi tööd häirivate tegevuste raames kasutatavate artefaktide kohta teabe ja koopiate saamist. Kui artefakt on kätte saadud, tuleb see läbi vaadata. See hõlmab artefaktide olemuse, töömehhanismide, versiooni ja kasutuse analüüsimist ning artefaktide tuvastamiseks, eemaldamiseks ja süsteemi nende eest kaitsmiseks sobivate reageerimisstrateegiate väljatöötamist (või soovitamist). Kuna erinevat tüüpi CSIRTides on artefaktide käsitlemine lahendatud erinevalt, saab seda teenust täpsemalt liigitada sooritatud tegevuste ja osutatud abi tüübi alusel.

Artefaktianalüüs

CSIRT uurib ja analüüsib kõiki arvutisüsteemist leitud artefakte. Analüüs võib hõlmata artefakti failitüübi ja struktuuri väljaselgitamist, uue artefakti võrdlemist olemasolevate artefaktide või sama artefakti muude versioonidega (et tuvastada võimalikud sarnasused ja erinevused) või koodi analüüsimist või osadeks lahutamist, et teha kindlaks artefakti otstarve ja funktsioon.

Artefaktidele reageerimine

See teenus hõlmab artefaktide süsteemist leidmiseks ja eemaldamiseks sobivate ja artefaktide installimist tõkestavate toimingute väljaselgitamist. Protsess võib hõlmata ka viirusetõrjetarkvarasse või IDSi lisatavate signatuuride loomist.

Artefaktidele reageerimise koordineerimine

See teenus hõlmab artefaktiga seotud analüüsitulemuste ja reageerimisstrateegiate sünteesimist ning teiste uurijate, CSIRTide, tootjate ja muude turbespetsialistidega jagamist. Tegevuste seas on teiste teavitamine ja tehnilise analüüsi sünteesimine paljude allikate põhjal. Samuti võivad tegevused hõlmata teadaolevate artefaktide, nende mõju ja vastavate reageerimisstrateegiate avaliku või kliendibaasi jaoks mõeldud arhiivi haldamist.

Proaktiivsed teenused

Proaktiivsete teenuste eesmärk on parendada kliendibaasi infrastruktuuri ja turbeprotsesse juba enne juhtumite või sündmuste ilmnemist või tuvastamist. Põhilised eesmärgid on juhtumite ärahoidmine ning siiski ilmnenud juhtumite mõju ja leviku piiramine.

Teadaanded

Teadaannete seas on näiteks sissetungihoiatused, haavatavustega seotud hoiatused ja turbenõuanded. Teadaanded teavitavad kliente uutest keskmise või pikaajalise mõjuga arengutest (nt vastleitud haavatavustest või sissetungiriistadest). Teadaannete abil saavad kliendid oma süsteeme ja võrke hiljuti leitud probleemide eest kaitsta veel enne, kui neid jõutakse ära kasutada.

Tehnoloogiaseire

Edaspidiste ohtude äratundmiseks seirab ja jälgib CSIRT uusi tehnilisi arenguid, sissetungijate tegevust ning muid sarnaseid suundumusi. Jälgimisse kaasatavate teemade valikut võib laiendada, et jälgida ka näiteks kohtuotsuseid, sotsiaalseid või poliitilisi ohtusid ning alles arengujärgus tehnoloogiaid. See teenus hõlmab turbealaste postitusloendite ja veebisaitide ning teadust, tehnikat, poliitikat või valitsust käsitlevate ajakohaste uudiste ja ajaleheartiklite lugemist, püsimaks kursis kliendibaasi süsteemide ja võrkude turvalisusega seotud teabega. Samuti võib see hõlmata suhtlemist teiste osapooltega, kes on vastavates valdkondades autoriteedid, et tagada parima ja täpseima teabe või tõlgenduse hankimine. Teenuse väljund võib olla näiteks keskmise või pikaajalise mõjuga turbeprobleeme käsitlevad teadaanded, juhendid või soovitused.

Turbeauditid või -hindamised

See teenus hõlmab asutuse turbeinfrastruktuuri üksikasjalikku läbivaatust ja analüüsi, võttes aluseks asutuse poolt või muude kohaldatavate standarditega määratletud nõuded. Samuti võib see hõlmata asutuse turbekäitumise läbivaatust. Auditeid ja hindamisi on väga mitmesuguseid. Siinkohal on neist ära toodud üksnes osa.

Infrastruktuuri läbivaatus

Riistvara- ja tarkvarakonfiguratsioonide, marsruuterite, tulemüüride, serverite ja töölauaseadmete füüsiline ülevaatamine, veendumaks, et need oleksid kooskõlas asutuse või IT-valdkonna heade tavade turbepoliitikate ja standardkonfiguratsioonidega.

Heade tavade kontrollimine

Töötajate ning süsteemi- ja võrguadministraatorite küsitlemine, et teha kindlaks, kas nende turbekäitumine vastab asutuses määratletud turbepoliitikale või teatud IT-standarditele.

Süsteemide skannimine

Haavatavus- ja viirusekontrollide kasutamine, et teha kindlaks, millised süsteemid ja võrgud on haavatavad.

Sissetungikontroll

Asukoha turvalisuse testimine süsteemide ja võrkude teadliku ründamise kaudu.
Selliste auditite või hindamiste korral on enne alustamist vaja saada asutuse juhtkonna nõusolek. Asutuse poliitika võib olla mõne neist lähenemisviisidest keelanud. Selle teenuse osutamine võib hõlmata ühtse tavadekomplekti väljatöötamist, mille suhtes teste või hindamisi läbi viiakse, ning testimise, hindamise, auditite või läbivaatustega tegelevate töötajate jaoks nõutavate oskuste või sertimisnõuete väljatöötamist. Selle teenuse osutamise võib edasi anda alltöövõtjale või hallatavale turbeteenuste pakkujale, kellel on auditite ja hindamiste läbiviimiseks nõutavad oskused.

Turbetööriistade, rakenduste, infrastruktuuride ja teenuste konfigureerimine ja haldamine

Selle teenuse raames selgitatakse välja või juhendatakse klienti selles, kuidas turvaliselt konfigureerida ja hallata CSIRTi kliendibaasi või CSIRTi enda kasutatavaid tööriistu, rakendusi ning üldist andmetöötluse infrastruktuuri. Lisaks juhendamisele võib CSIRT uuendada turbetööriistade ja -teenuste (nt IDS, võrgukontrolli- või seiresüsteemid, filtrid, pakendid, tulemüürid, virtuaalsed privaatvõrgud (VPNid) või autentimismehhanismid) konfiguratsiooni ning neid hooldada. CSIRT võib neid teenuseid osutada ka oma põhitöö raames. Samuti võib CSIRT vastavalt turbejuhistele konfigureerida ja hooldada servereid, lauaarvuteid, sülearvuteid, pihuarvuteid (PDAsid) ja muid raadiosideseadmeid. Kui konfiguratsioonide osas ilmneb probleeme või kui kasutusel on tööriistu või rakendusi, mis võivad CSIRTi hinnangul jätta süsteemi sissetungile haavatavaks, hõlmab see teenus ka vastavate probleemide haldamist.

Turbetööriistade väljatöötamine

See teenus hõlmab uute kliendikohaste tööriistade väljatöötamist, mida vajavad või soovivad kliendid või CSIRT ise. Muu hulgas võib see tähendada näiteks klientide kasutatava kohandatud tarkvara jaoks turvapaikade väljatöötamist või turvaliste tarkvaradistributsioonide koostamist, mida saab kasutada rünnakus kahjustatud hostide taastamiseks. Samuti võib see hõlmata selliste tööriistade või skriptide väljatöötamist, mis laiendavad olemasolevate turbetööriistade funktsionaalsust – näiteks teatud haavatavuse parandav lisandmoodul või võrgukontrollirakendus, krüptimistehnika kasutamist hõlbustavad skriptid või automatiseeritud paigalevitusmehhanismid.

Sissetungituvastusteenused

Seda teenust osutavad CSIRTid vaatavad läbi olemasolevaid IDSi logisid, analüüsivad teatud kindlale lävele vastavaid sündmusi ja algatavad sündmustele reageerimise või saadavad kõik teated edasi vastavalt eelmääratletud teenindustaseme lepingule või eskalatsioonistrateegiale. Sissetungituvastus ja sellega seostuvate turbelogide analüüsimine võib olla üpris hirmutav ülesanne – ei piirdu see ju üksnes sellega, kuhu keskkonnas vajalikud andurid paigutada, vaid hõlmab ka andmete kogumist ja suurte andmemahtude analüüsimist. Sageli on teabe sünteesimiseks ja tõlgendamiseks vaja eritööriistu või -oskusi, et tunda ära valehäireid, rünnakud või võrgusündmused ning võtta kasutusele selliste sündmuste ärahoidmiseks või minimeerimiseks vajalikud strateegiad. Mõnes asutuses eelistatakse see teenus sisse osta mujalt, näiteks hallatava turbeteenuse pakkujatelt, kellel on selliste teenuste osutamisel rohkem kogemusi.

Turbealase teabe levitamine

See teenus annab klientide käsutusse laiahaardelise ja hõlpsasti leitava kasuliku teabe kollektsiooni, millest on turvalisuse suurendamisel kindlasti abi. See teave võib sisaldada järgmist:

- CSIRTi teavitamise juhiseid ja kontaktteavet;
- teadete, hoiatuste ja muude teadaannete arhiive;
- praegu kehtivate heade tavade dokumentatsiooni;
- üldisi arvutiturbe suuniseid;
- poliitikaid, protseduure ja kontrollnimekirju;
- paigaarendus ja -levitusteavet;
- tootjate veebisaitide linke;
- juhtumiteavituse praegust statistikat ja suundumusi;
- muud teavet, millest võib üldise turbekäitumise parendamisel kasu olla.

Seda teavet võib välja töötada ja avaldada nii CSIRT ise kui ka mõni muu sama asutuse osakond (IT, personaliosakond või avalike suhete osakond) ning see võib hõlmata ka välistest allikatest (teistelt CSIRTidelt, tootjatelt ja turbespetsialistidelt) pärinevat teavet.

Turbekvaliteedi halduse teenused

Sellesse kategooriasse jäävad teenused, mis pole konkreetselt seotud ainult juhtumite töötlemise või CSIRTidega. Pigem on need tuntud ja juba ammu sisse töötatud teenused, mille eesmärk on asutuse üldise turvalisuse suurendamine. Kasutades ära eelkirjeldatud reaktiivsete ja proaktiivsete teenuste osutamisel saadud kogemusi, võib CSIRT lisada kvaliteedihaldusteenustele uusi võimalusi ja vaatenurki. Need teenused on loodud hõlmama tagasisidet ja õppetunde, mis on omandatud juhtumitele, haavatavustele ja rünnakutele reageerimisel saadud teadmiste põhjal. Selliste kogemuste lisamine turbekvaliteedi halduse protsessi osana traditsiooniliste teenuste koosseisu (neid on kirjeldatud allpool) võib asutuse pikaajalisi turbemeetmeid märgatavalt parendada. Sõltuvalt sellest, millised on asutuse vastutusalad ja ülesehitus, võib CSIRT neid teenuseid ise osutada või anda oma panuse terve asutuse ühistesse jõupingutustesse. Järgmistes lõikudes kirjeldatakse, kuidas võib CSIRTi kogemustest nende turbekvaliteedi halduse teenuste osas abi olla.

Riskianalüüs

CSIRTid võivad anda lisaväärtust nii riskianalüüsi- kui ka riskihindamisteenustele. See aitab asutusel paremini hinnata tegelikke ohtusid, koostada realistlikke kvalitatiivseid ja kvantitatiivseid hinnanguid teabevara ohustavatest riskidest ning teha ülevaateid kaitse- ja reageerimisstrateegiatest. Seda teenust osutavad CSIRTid viiksid läbi uute süsteemide ja äriprotsesside riskianalüüsitegevusi (või aitaksid selliste tegevuste läbiviimisel kaasa) või hindaksid kliendibaasi varade ja süsteemide vastu suunatud ohte ja rünnakuid.

Majandustegevuse jätkamise ja tõrgete kõrvaldamise kavandamine

Võttes aluseks seni aset leidnud sündmused ja uute juhtumi- või turbesuundumuste prognoosid, võib üsna kindlalt väita, et aina suurem osa juhtumitest võib ettevõtte tegevust tõsiselt kahjustada. Seetõttu tuleks majandustegevuse jätkumise tagamiseks sellistele juhtumitele parima reageerimisviisi kavandamisel CSIRTi kogemusi ja soovitusi kindlasti arvesse võtta. Seda teenust osutavad CSIRTid on majandustegevuse jätkumise ja õnnetuseohje kavandamisse kaasatud vähemalt nende sündmuste osas, mis on seotud arvutiturbe alaste ohtude ja rünnakutega.

Turbealane nõustamine

CSIRTid saavad kliendibaasile pakkuda nende majandustegevuse jaoks kõige paremini sobiva turbekäitumise alast nõustamise ja suuniseid. Seda teenust osutav CSIRT on kaasatud uute süsteemide, võrguseadmete, tarkvararakenduste või tervet ettevõtet hõlmavate äriprotsesside ostmise, installimise või turvamise jaoks vajalike eeltingimuste väljaselgitamisse või soovituste ettevalmistamisse. See teenus hõlmab asutuse või kliendibaasi turbepoliitikate väljatöötamise juhendamist ja abi osutamist. Samuti võib see hõlmata seadusandlikele organitele või muudele riigiorganitele tunnistuste ja nõuannete pakkumist.

Teadlikkuse suurendamine

CSIRTid oskavad hinnata, millistes valdkondades vajavad kliendid üldaktsepteeritud turbekäitumise ja asutuse turbepoliitikate järgimiseks rohkem teavet ja juhendamist. Kliendibaasi üldise turbealase teadlikkuse suurendamine aitab neil paremini mõista turbega seotud probleeme ja ka igapäevatoiminguid sooritada senisest turvalisemalt. See võib vähendada õnnestunud rünnakute sagedust ja suurendada tõenäosust, et kliendid oskavad ise rünnakuid avastada ja nendest teatada. See omakorda vähendab reageerimiseks kuluvat aega ja elimineerib või minimeerib kahjud.
Seda teenust osutavad CSIRTid otsivad võimalusi turbealase teadlikkuse suurendamiseks, koostades artikleid, plakateid, infolehti, veebisaite või muid teaberessursse, mis selgitavad turbealaste heade tavade vajalikkust, pakuvad kasulikke nõuandeid ja kirjeldavad võimalikke ettevaatusabinõusid. Samuti võib seda teenust osutav CSIRT korraldada koosolekuid ja seminare, et hoida kliente kursis pidevalt uuendavate turbeprotseduuride ja asutuse IT-süsteemide vastu suunatud ohtudega.

Haridus/koolitus

See teenus hõlmab klientidele arvutiturbega seotud probleemide kohta teabe andmist seminaride, töötubade, kursuste ja õppetükkide kaudu. Käsitletavate teemade seas võivad olla juhtumitest teavitamise juhised, sobivad reageerimisviisid, juhtumitele

reageerimise tööriistad, juhtumite ärahoidmise võimalused ning muu teave, mis on vajalik arvutisüsteemide kaitsmiseks ja arvutiturbe juhtumite avastamiseks, neist teavitamiseks ja neile reageerimiseks.

Tootehindamine või -sertifitseerimine

Selle teenuse osutamisel võib CSIRT läbi viia tööriistade, rakenduste või muude teenuste tootehindamise, et tagada toodete turvalisus ja vastavus aktsepteeritud CSIRTi või asutuse turbepoliitikatele. Hinnatavad tööriistad ja rakendused võivad olla nii avatud lähtekoodiga kui ka kommertstooted. Seda teenust võidakse osutada nii hinnangu koostamisena kui ka mõne sertifitseerimisprogrammi raames, sõltuvalt asutuses või CSIRTi poolt kasutusele võetud standarditest.

A.3 Näited

Fiktiivne CSIRT

0. etapp: CSIRT olemuse mõistmine

Näidis-CSIRT peab teenindama keskmise suurusega asutust, kus töötab kuni 200 inimest. Asutusel on oma IT-osakond ja veel kaks harukontorit samas riigis. Infotehnoloogial on ettevõtte jaoks oluline roll, kuna seda kasutatakse ettevõttesisese suhtluse, andmevõrgu ja ööpäev läbi töötava e-äri jaoks. Asutusel on oma võrk ja liiasühendus Internetiga kahe erineva Interneti-teenuse pakkuja kaudu.

- -

1. etapp: alustamine

Algfaasis kavandatakse uus CSIRT ettevõttesisese CSIRTina, mis osutab teenuseid töörühma majutavale ettevõttele, kohalikule IT-osakonnale ja töötajatele. Samuti toetab ja koordineerib see eri harukontorite IT-turbega seotud juhtumite käsitlemist.

- -

2. etapp: õigete teenuste valimine

Projekti algetapis otsustatakse, et uus CSIRT keskendub peamiselt asutuse töötajatele teatud põhiteenuste pakkumisele.

Otsustatakse, et pärast pilootetappi kaalutakse pakutavate teenuste valiku laiendamist ja on võimalik, et valikusse lisatakse ka turbehaldusteenused. Selle otsuse tegemisel lähtutakse pilootprojektis osalenud klientidelt saadud tagasisidest ja kvaliteedikontrolli osakonnaga tehtud tihedast koostööst.

- -

3. etapp: kliendibaasi ja sobivate sidekanalite analüüsi koostamine

Ajurünnak, kus osalesid teatud võtmeisikud juhtkonnast ja kliendibaasist, andis piisavalt lähteandmeid SWOT-analüüsi jaoks. Jõuti järeldusele, et klientide seas valitseb vajadus põhiteenuste järele:

- teated ja hoiatused;
- juhtumite käsitlemine (analüüs, reageerimistugi ja reageerimise koordineerimine);
- teadaanded.

Teabe levitamine peab olema hästi korraldatud, et teave jõuaks võimalikult suure osani kliendibaasist. Seetõttu võeti vastu otsus, et teated, hoiatused ja teadaanded (turbenõuannete kujul) avaldatakse nii vastaval veebisaidil kui ka postitusloendi kaudu levitades. CSIRT kasutab juhtumiteadete vastuvõtmiseks e-posti, telefoni ja faksi. Järgmises etapis kavatsetakse kasutusele võtta ühtne veebivorm.

4. etapp: missiooni sõnastamine

Fiktiivse CSIRTi juhtkond on koostanud järgmise missiooni kirjelduse:
„Fiktiivne CSIRT pakub töörühma majutava ettevõtte töötajatele teavet ja abi proaktiivsete meetmete kasutuselevõtul, vähendamaks arvutiturbega seotud juhtumite ohtu ning reageerimaks sellistele juhtumitele, kui neid siiski esineb.“

Sellega väljendab fiktiivne CSIRT selgelt, et tegemist on asutusesisese CSIRTiga, mille põhitegevus seisneb IT-turbega seotud probleemide lahendamises.

- -

5. etapp: äriplaani määratlemine

Finantsmudel

Kuna ettevõttel on ööpäev läbi töötav e-äri ja samuti ööpäev läbi töötav IT-osakond, on jõutud otsusele osutada tööajal täiskomplekti teenuseid ning väljaspool tööaega töötada väljakutsepõhiselt. Kliendibaasile osutatakse teenuseid tasuta, kuid projekti piloot- ja hindamisetapis analüüsitakse võimalust osutada teenuseid ka välisklientidele.

Tulumudel

Projekti algusjärgus ja pilootetapi ajal finantseeritakse CSIRTi tegevust seda majutava ettevõtte kaudu. Piloot- ja hindamisetapis arutatakse täiendavaid finantseerimisvõimalusi (sh võimalust müüa teenuseid välisklientidele).

Organisatsioonimudel

Kuna töörühma majutav asutus on väikeettevõte, on valitud integreeritud mudel.
Tööajal osutab kolmest töötajast koosnev personal põhiteenuseid (turbenõuannete levitamine ja juhtumite käsitlemine/koordineerimine).

Vajalike oskustega inimesed on ettevõtte IT-osakonnas juba olemas. Selle osakonnaga sõlmitakse kokkulepe, mille alusel saab uus CSIRT vajaduse korral ajutist abi taotleda. Lisaks saab kasutada IT-osakonna väljakutsete alusel töötavaid tehnikuid.
CSIRTi põhimeeskonnas hakkab töötama neli täiskohaga inimest; lisaks annab CSIRT tööd veel viiele inimesele. Üks neist on nõus töötama erinevates vahetustes.

Töötajad

CSIRTi meeskonnajuhil on kogemusi IT-turbe vallas. Samuti on ta töötanud esimese ja teise taseme tugiteenuseid osutavas asutuses ja paindliku kriisihalduse valdkonnas. Ülejäänud kolm meeskonnaliiget on turbespetsialistid. Osalise tööajaga töötavad CSIRTi liikmed, kelle põhitöökoht on IT-osakonnas, on ettevõtte infrastruktuuri osas oma ala spetsialistid.

5. etapp: kontori kasutuselevõtt ja infoturbepoliitika

Kontoriseadmed ja asukoht

Kuna töörühma majutaval ettevõttel on füüsiline turvalisus juba tõhusalt paigas, ei pea uus CSIRT selle pärast muretsema. Tegevuse koordineerimiseks hädaolukorras seatakse sisse nn staap. Krüptimismaterjalide ja tundliku loomuga dokumentide hoidmiseks ostetakse seif. Sisse on seatud eraldi telefoniliin, sh kommutaator, mis võimaldab kasutada sama telefoninumbrit tööajal infoliini teenindamiseks ja väljaspool tööaega väljakutseid ootava töötaja mobiiltelefoni ühendamiseks.

CSIRTiga seotud teabe avaldamiseks võib kasutada ka ettevõtte veebisaiti ja olemasolevaid seadmeid. Installitakse postitusloendi tarkvara, mille piiratud juurdepääsuga osa on mõeldud meeskonnaliikmete omavaheliseks suhtluseks ja teiste meeskondadega suhtlemiseks. Andmebaasis hoitakse kõigi töötajate kontaktandmeid; kontaktandmete väljaprinti hoitakse seifis.

Eeskirjad

Kuna CSIRT on integreeritud ettevõttega, millel on infoturbepoliitika juba olemas, on vastav poliitika ettevõtte juristi abiga välja töötatud ka CSIRTi jaoks.

- -

7. etapp: koostöövõimaluste otsimine

ENISA veebilehe jaotise *Inventory* kaudu õnnestus kiiresti üles leida mitu samas riigis tegutsevat CSIRTi, kellega võeti ühendust. Vastne meeskonnajuht korraldas ühe CSIRTiga kokkusaamise. Lisaks koosolekul osalemisele saadi teavet riiklike CSIRTi tegevuse kohta.

Koosolek osutus erakordselt kasulikuks: koguti näiteid töömeetodite kohta ja saadi abi mitmelt muult töörühmalt.- -

8. etapp: äriplaani edendamine

Vastu on võetud otsus koguda seiku ja näitajaid ettevõtte senisest tegevusest. IT-turbe olukorrast statistilise ülevaate loomiseks on see äärmiselt kasulik. Statistika ajakohasena hoidmiseks tuleks teabe kogumist jätkata ka siis, kui CSIRT on juba loodud ja töötab.

Ühendust võeti muude riiklike CSIRTidega, kellega vahetati investeeringupõhjenduste koostamise osas kogemusi. CSIRTid olid nõu ja jõuga igati abiks, koostades slaide teabega IT-turbega seotud juhtumite viimase aja arengu ja juhtumitega kaasnevate kulude kohta.

Käesoleva dokumendi näidetes kasutatava fiktiivse CSIRTi puhul polnud vaja ettevõtte juhtkonda IT-äri olulisuses veenda ja seetõttu oli projekti alustamiseks loa saamine üsna lihtne. Ette valmistati investeeringupõhjendus ja projektikava (sh hinnang nii asutamisega kaasnevate kulude kui ka tegevuskulude kohta).

- -

9. etapp: protsessivoogude ning tehniliste ja tööprotseduuride sisseseadmine
Fiktiivne CSIRT keskendub CSIRTi põhiteenuste osutamisele:

- teated ja hoiatused;
- teadaanded;
- juhtumitöötlus.

Töörühmas on välja töötatud hästi toimivad protseduurid, millest saavad hõlpsasti aru kõik töörühma liikmed. Samuti on fiktiivne CSIRT palganud õiguseksperdi, kes tegeleb vastutusega seotud küsimuste ja infoturbepoliitikaga. Töörühm on kasutusele võtnud mitu kasulikku tööriista ja saanud teiste CSIRTidega nõu pidades vajalikku teavet tööga seotud küsimuste kohta.

Loodud on ühtne mall turbenõuannete ja juhtumiaruannete jaoks. Juhtumite käsitlemiseks kasutab töörühm RTIRi.

- -

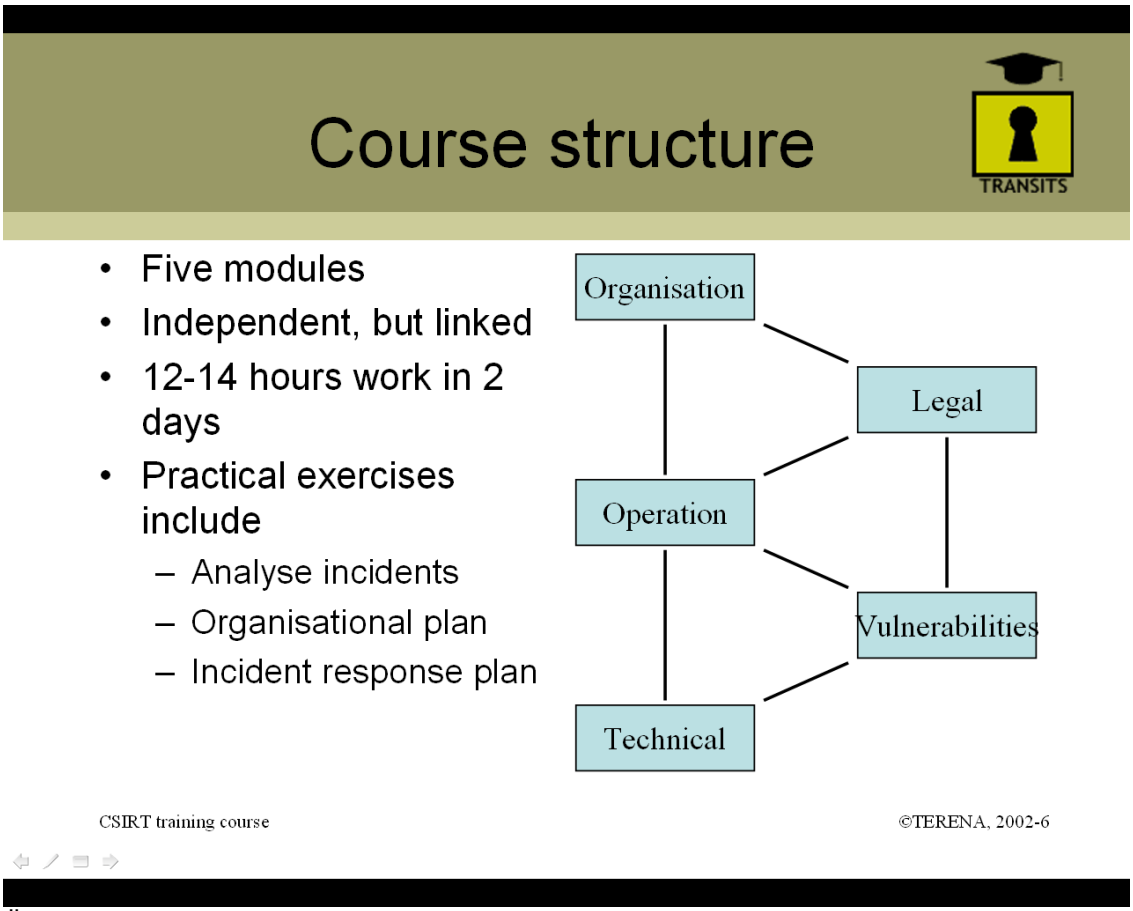
10. etapp: töötajate koolitamine
Fiktiivne CSIRT otsustab saata kõik tehnilised töötajad järgmistele pakutavatele TRANSITSi kursustele. Meeskonnajuht osaleb lisaks ka CERT/CC kursusel *CSIRTi juhtimine*.

- -

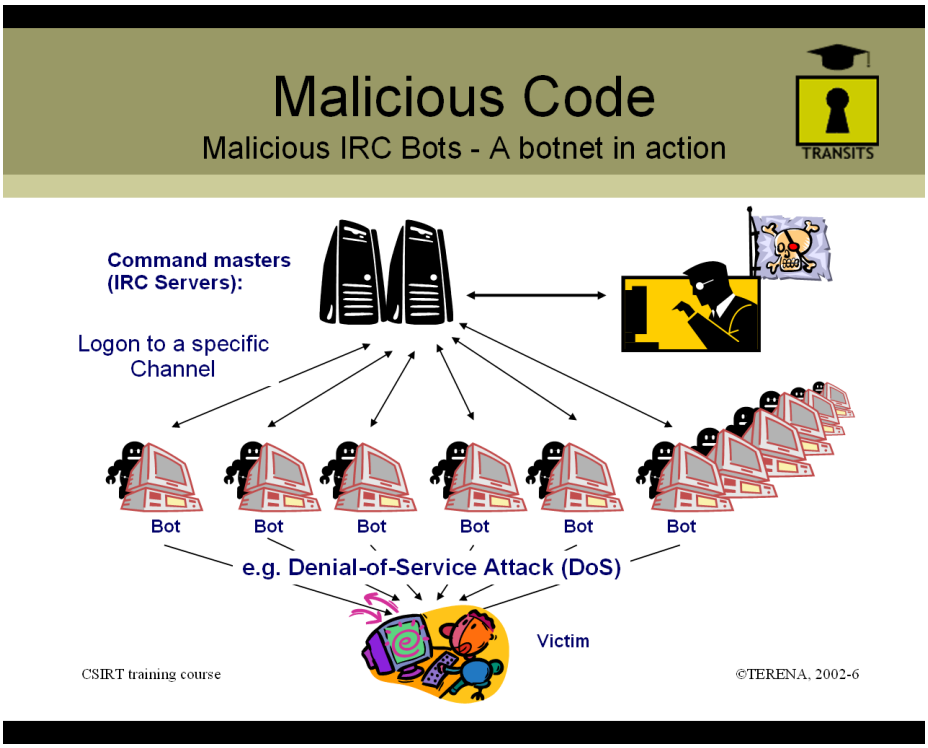
11. etapp: harjutused
Paari esimese töönädala jooksul kasutas fiktiivne CSIRT harjutamiseks mitut fiktiivset juhtumit (need saadi näidetena teistelt CSIRTidelt). Lisaks anti välja mitu turbenõuannet, mis põhinesid riist- ja tarkvaratootjatelt saadud tegelikul haavatavuse teabel. CSIRTi töötajad kohandasid selle teabe oma kliendibaasi vajadustele vastavaks.

A.4 CSIRTi kursuste näidismaterjal

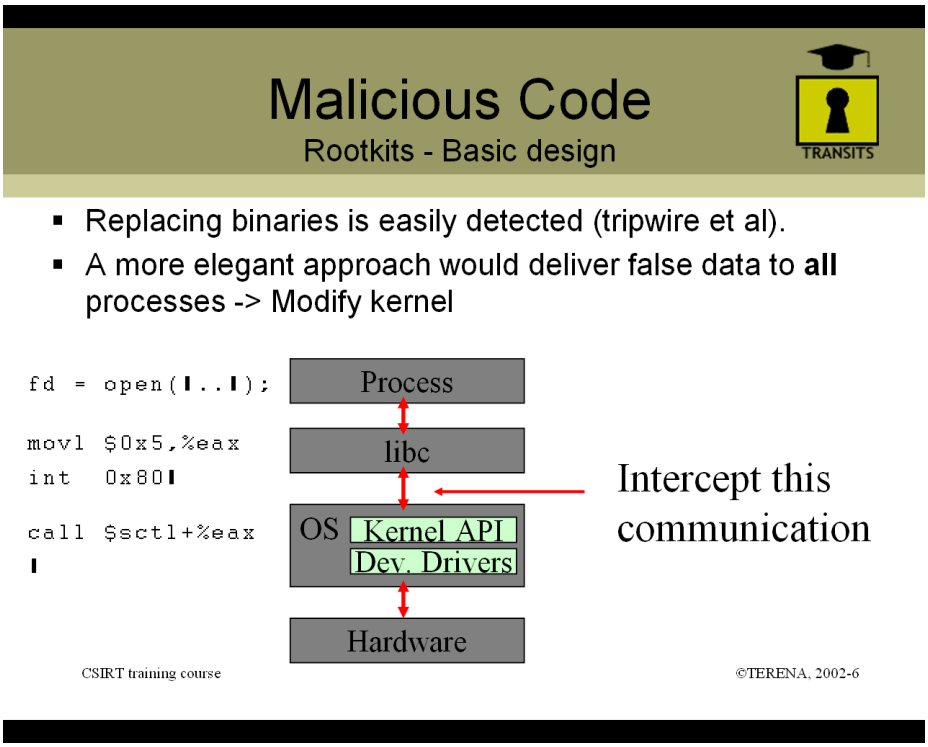
TRANSITS (Terena lahkel loal: http://www.terena.nl)



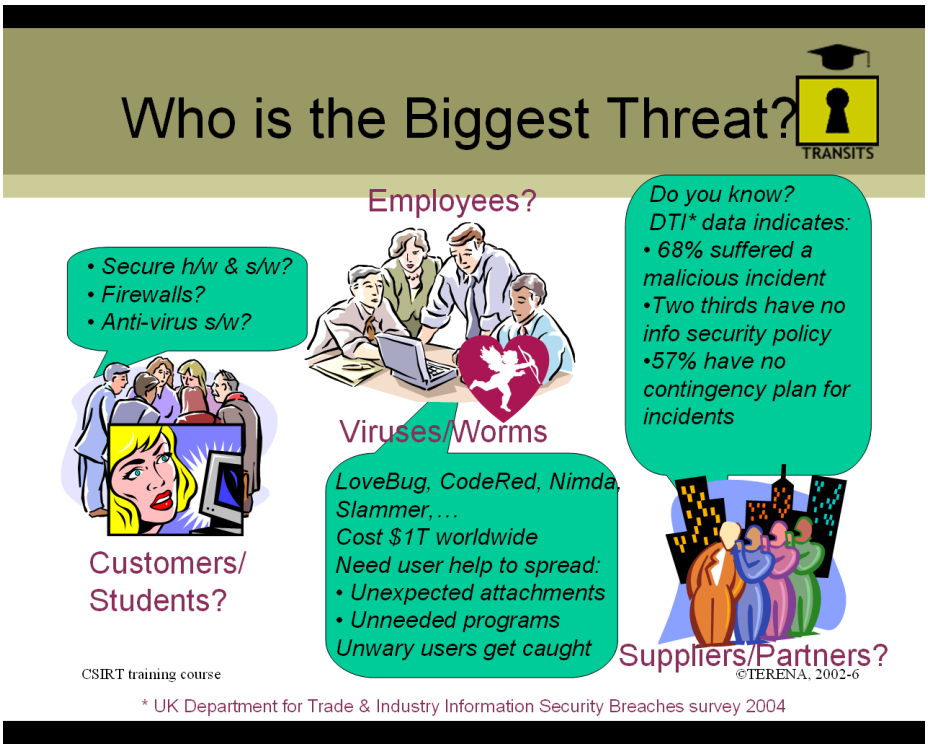
Ülevaade: kursuse ülesehitus



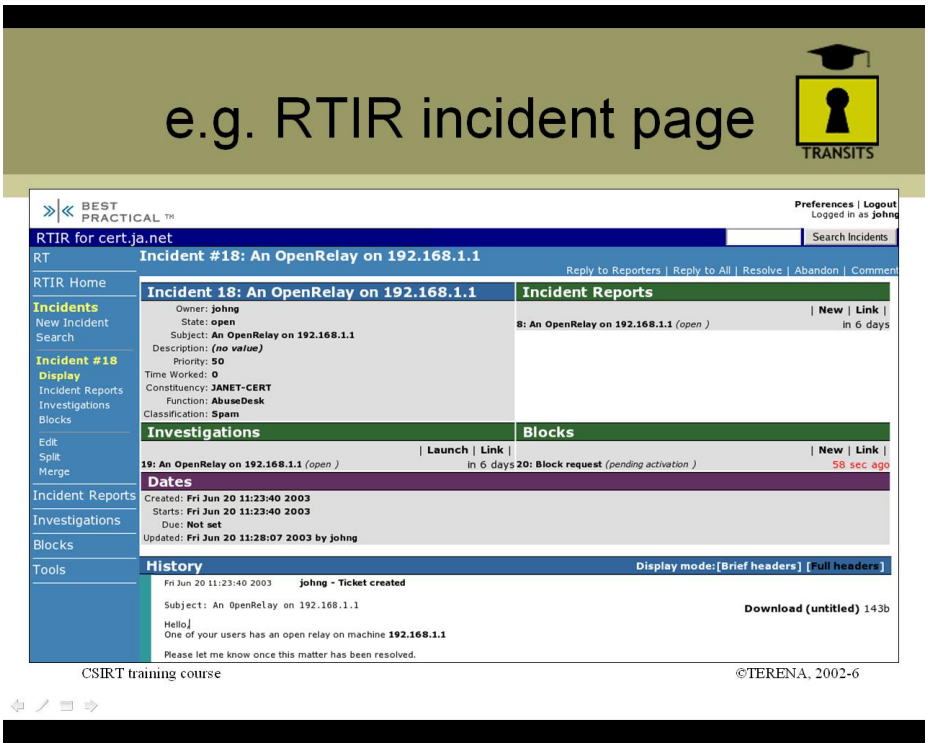
Tehniline moodul: *botnet*-võrgu kirjeldus



Tehniline moodul: *rootkit*-programmi baasdisain



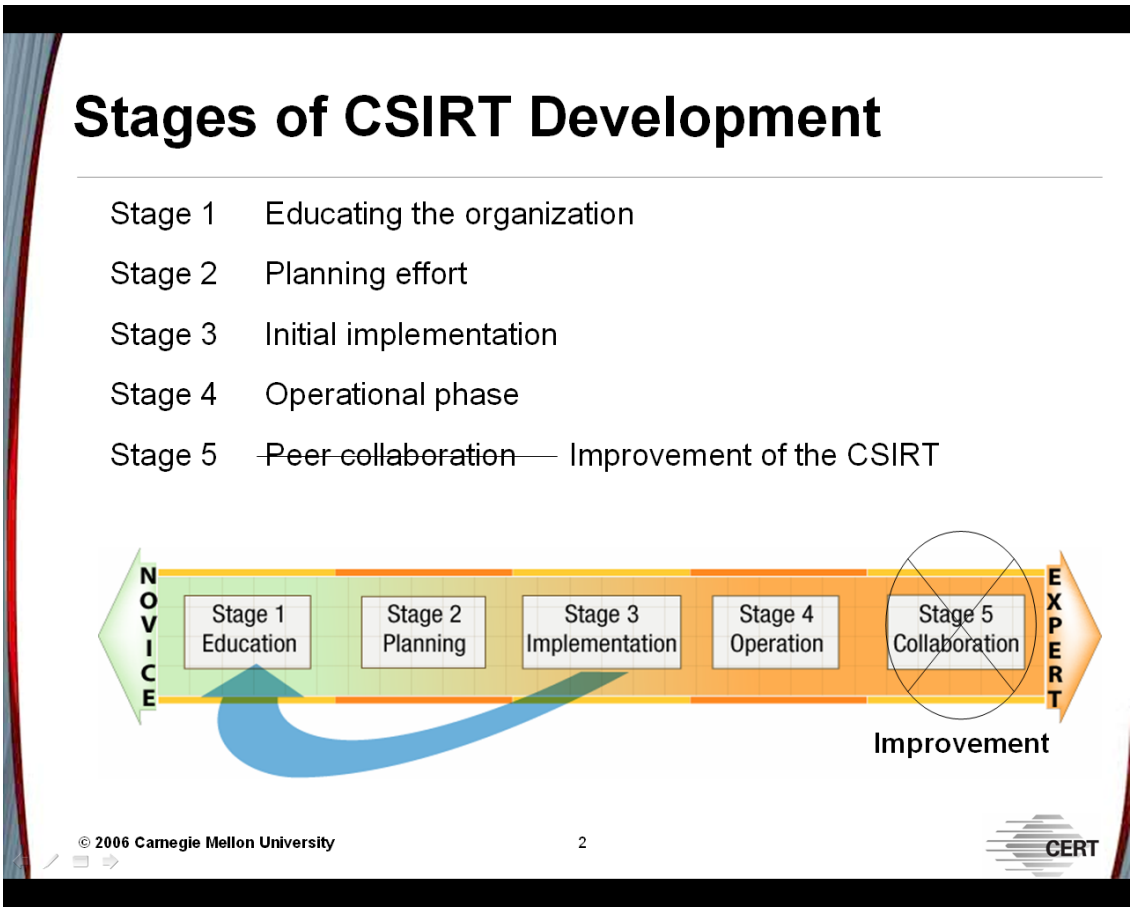
Organisatsioonimoodul: insaider või autsaider – kas suurem oht tuleb seest või väljast?



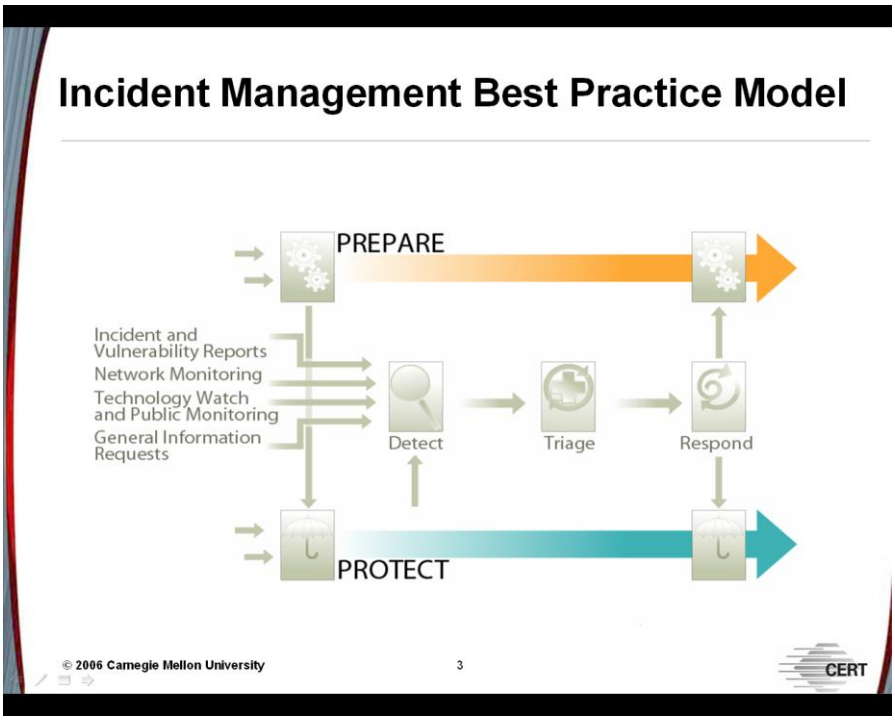
Juhtumi jälgimine:– Request Tracker for Incident Response (RTIR)

„CSIRTide sisseseadmine“ (CERTi/CC lahkel loal: http://www.cert.org)

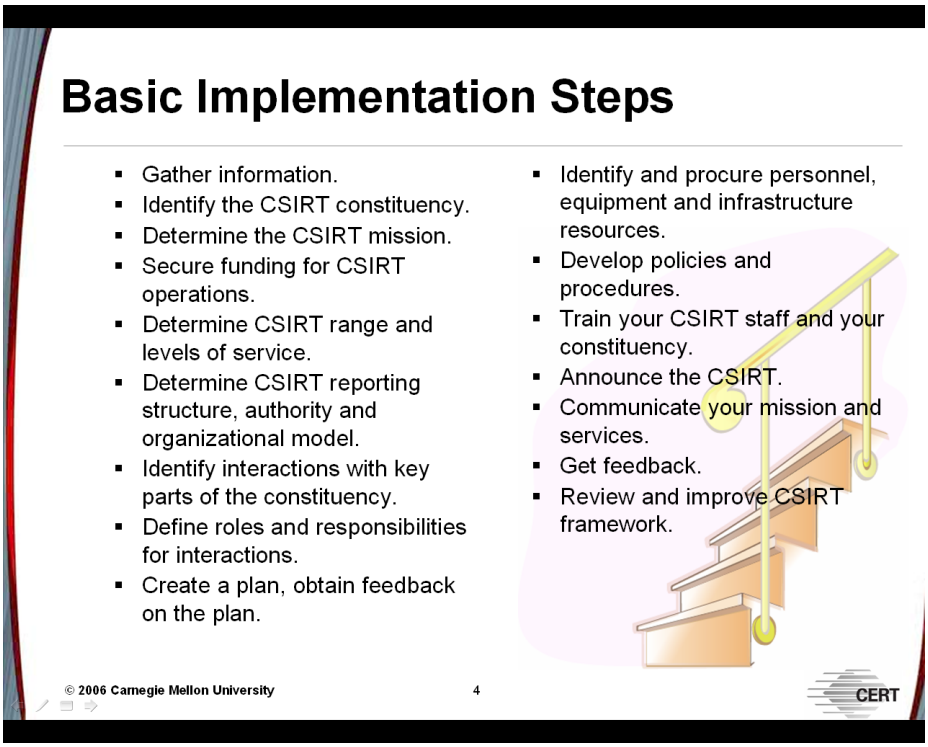
ENISA avaldab tänu CERTi kava CSIRTide arendusrühmale, kes lubas meil kasutada oma koolituskursuste sisu.



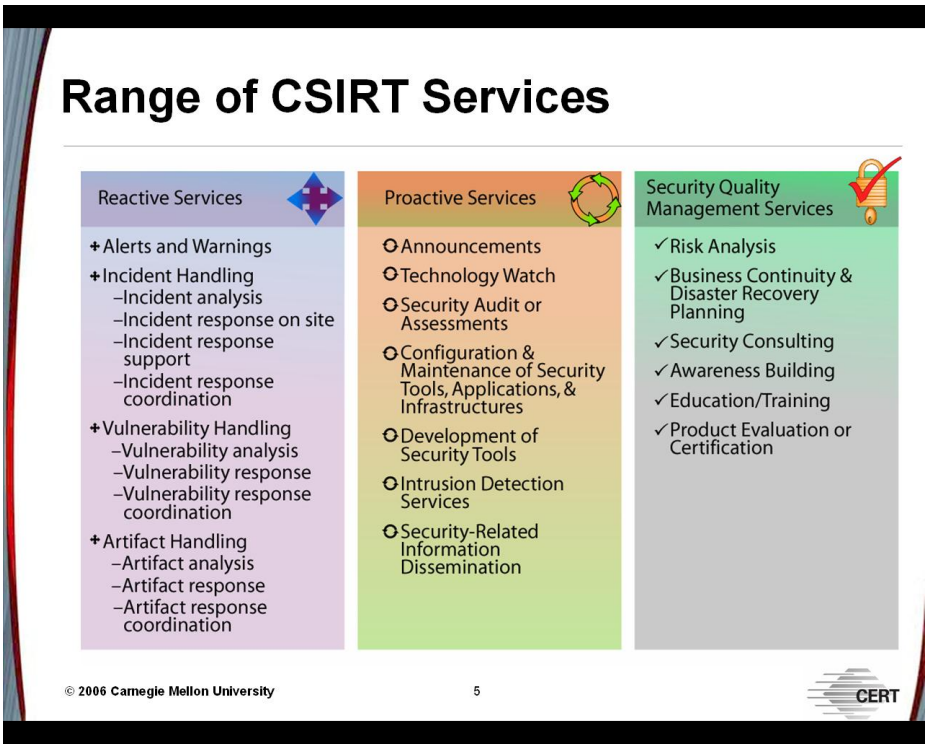
Näide CERTi/CC koolituskursusest: CSIRTi asutamise etapid



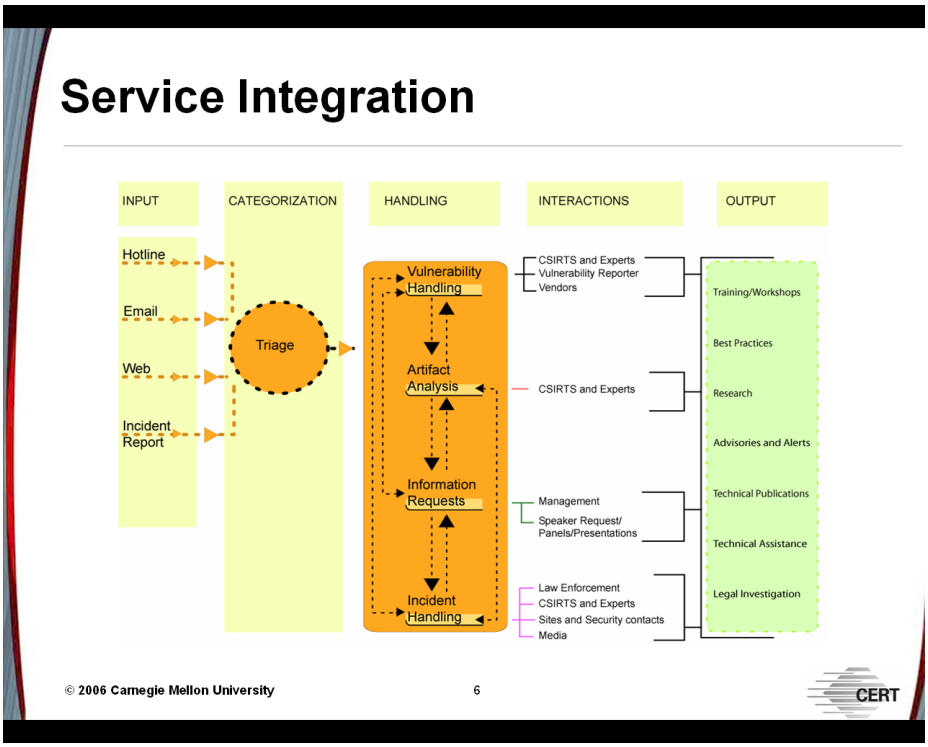
Näide CERTi/CC koolituskursusest: juhtumihalduse head tavad



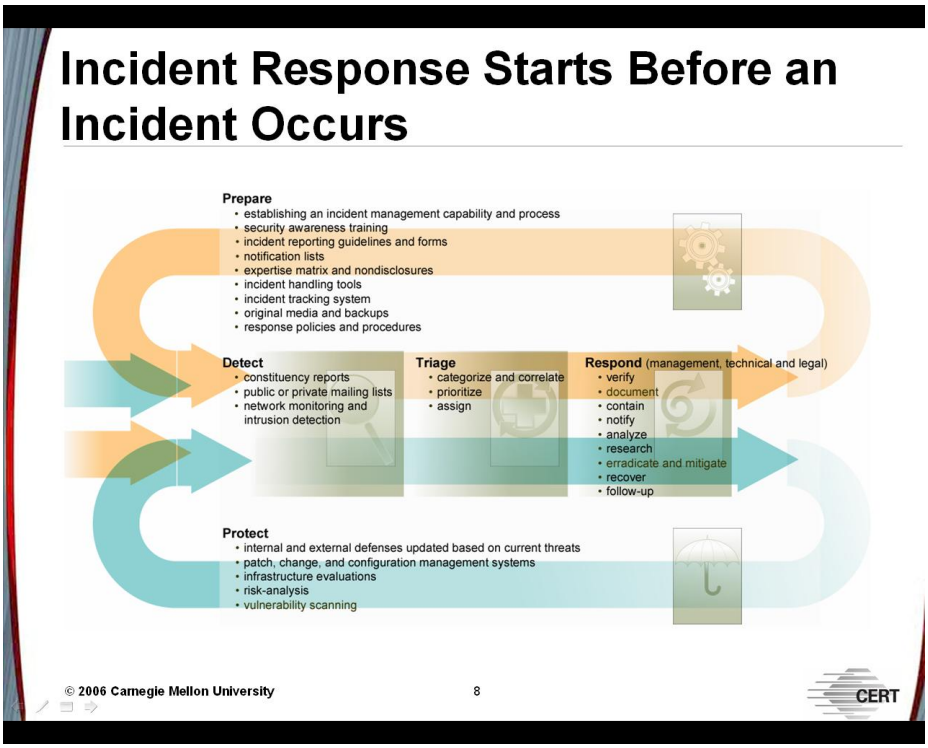
Näide CERTi/CC koolituskursusest: CSIRTi asutamisel vajalikud toimingud



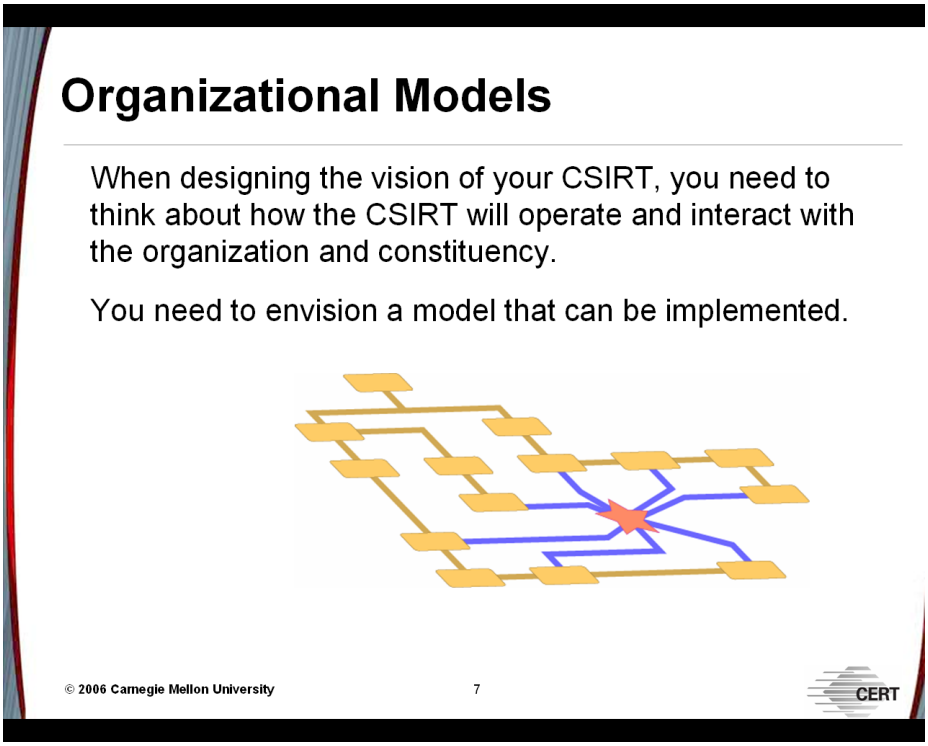
Näide CERTi/CC koolituskursusest: teenused, mida CSIRT võib osutada



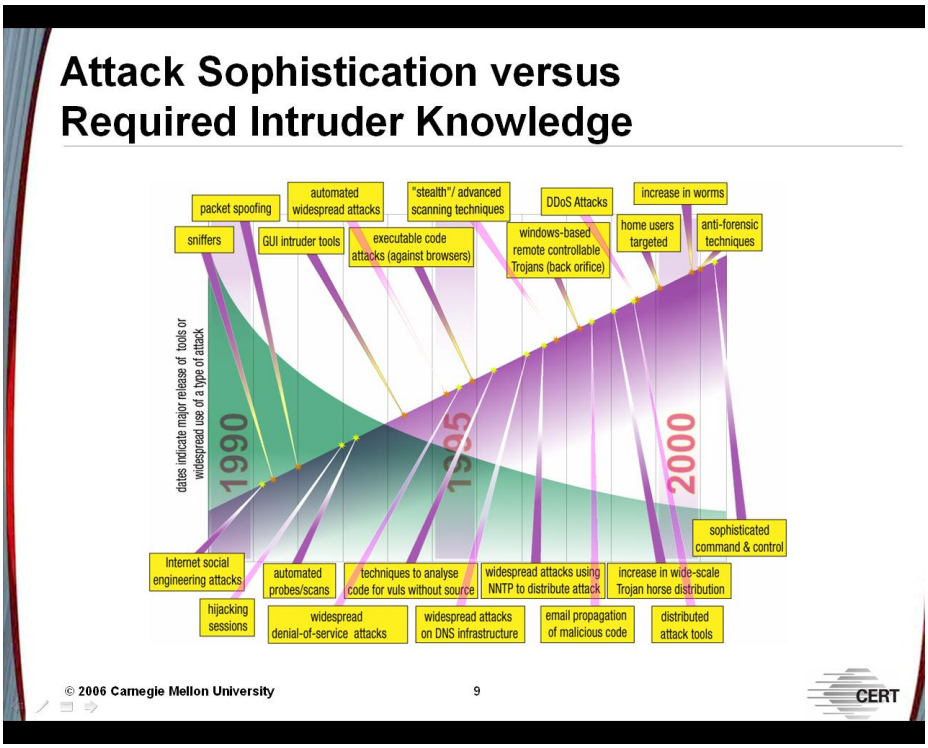
Näide CERTi/CC koolituskursusest: juhtumihalduse töövoog



Näide CERTi/CC koolituskursusest: juhtumile reageerimine



Näide CERTi/CC koolituskursusest: kuidas tuleks CSIRTi korraldada?



Näide CERTi/CC koolituskursusest: rohkem teadmisi, väiksemad kahjud