



VAIHEITTAINEN LÄHESTYMISTAPA CSIRT- TIETOTURVARYHMÄN PERUSTAMISEEN

Suorite WP2006/5.1(CERT-D1/D2)

Sisällysluettelo

1	Yhteenveto	2
2	Oikeudellinen huomautus	2
3	Kiitokset	2
4	Johdanto	3
4.1	KOHDERYHMÄ	4
4.2	ASIAKIRJAN KÄYTTÖ	4
4.3	ASIAKIRJAN RAKENNE	5
5	CSIRT-ryhmän suunnittelun ja perustamisen yleinen strategia	6
5.1	MIKÄ ON CSIRT?	6
5.2	CSIRT-RYHMÄN MAHDOLLISET PALVELUT	10
5.3	ASIAKASKUNNAN ANALYSOINTI JA TOIMENKUVAN MÄÄRITTÄMINEN	12
6	Liiketoimintasuunnitelman laatiminen	18
6.1	RAHOITUSMALLIN MÄÄRITTÄMINEN	18
6.2	ORGANISAATORAKENTEEN MÄÄRITTÄMINEN	20
6.3	OIKEAN HENKILÖSTÖN PALKKAAMINEN	24
6.4	TOIMISTON KÄYTTÖ JA LAITTEISTO	26
6.5	TIETOTURVAPOLITIIKAN LAATIMINEN	28
6.6	YHTEISTYÖMAHDOLLISUUDET MUIDEN CSIRT-RYHMIEN JA MAHDOLLISTEN KANSALLISTEN ALOITTEIDEN KANSSA	29
7	Liiketoimintasuunnitelman edistäminen	31
7.1	LIIKETOIMINTASUUNNITELMIEN KUVAUS JA JOHDON KANNUSTAMINEN TOIMIMAAN	32
8	Esimerkkejä toiminnallisista ja teknisistä menettelyistä (työnkulku)	36
8.1	ASIAKASKUNNAN IT-JÄRJESTELMÄN ARVIOIMINEN	37
8.2	HÄLYTYSTEN, VAROITUSTEN JA TIEDOTTEIDEN TUOTTAMINEN	38
8.3	TIETOTURVALOUKKAUSTEN KÄSITTELY	44
8.4	ESIMERKKI KÄSITTELYAIKATAULUSTA	50
8.5	KÄYTETTÄVISSÄ OLEVAT CSIRT-TYÖKALUT	51
9	CSIRT-koulutus	53
9.1	TRANSITS	53
9.2	CERT/CC	54
10	Käytännön harjoitus: tietoturvatiedotteen laatiminen	55
11	Päätelmät	60
12	Hankesuunnitelman kuvaus	61
LIITE		63
A.1	LISÄLUKEMISTA	63
A.2	CSIRT-PALVELUT	64
A.3	ESIMERKIT	73
A.4	ESIMERKKIAINEISTOA CSIRT-KURSSEILTA	77

1 Yhteenveto

Tässä asiakirjassa kuvataan tietoturvaloukkauksia käsittelevän ryhmän (Computer Security and Incident Response Team, CSIRT) perustamista kaikista asiaan liittyvistä näkökulmista, kuten liikkeenjohdon, prosessihallinnan ja tekniikan näkökulmasta. Tällä asiakirjalla pannaan täytäntöön Euroopan verkko- ja tietoturvaviraston (ENISA) vuoden 2006 työohjelman luvussa 5.1 esitetyt kaksi suoritetta:

- Tämä asiakirja: *Kirjallinen kertomus CERT-ryhmän tai vastaavien ryhmien perustamista koskevasta vaiheittaisesta lähestymistavasta esimerkkitapauksineen. (CERT-D1)*
- Luku 12 ja ulkoiset tiedostot: *Ote menettelyohjeista eritellyssä muodossa menettelyohjeiden soveltamisen helpottamiseksi käytännössä. (CERT-D2)*

2 Oikeudellinen huomautus

Tämä julkaisu ilmentää julkaisun laatijoiden ja julkaisijoiden näkemyksiä ja tulkintoja, ellei toisin ole mainittu. Sitä ei pidä tulkita ENISAn tai sen elinten toteuttamaksi toimeksi siltä osin kuin sitä ei ole toteutettu Euroopan verkko- ja tietoturvaviraston perustamisesta annetun asetuksen (EY) N:o 460/2004 mukaisesti. Julkaisu ei ole välttämättä viimeisimmän kehityksen mukainen, ja julkaisua voidaan päivittää ajoittain.

Ulkoisiin lähteisiin viitataan soveltuvien osin. ENISA ei ole vastuussa ulkoisen lähteiden sisällöstä, julkaisussa mainitut ulkoiset verkkosivut mukaan luettuina.

Julkaisu on tarkoitettu ainoastaan opetus- ja tiedotuskäyttöön. ENISA tai sen nimissä toimiva henkilö ei ole vastuussa julkaisun sisältämän tiedon mahdollisesta käytöstä.

Kaikki oikeudet pidätetään. Tätä julkaisua ei saa jäljentää, tallentaa tietojärjestelmään tai siirtää muilla keinoin sähköisesti tai mekaanisesti, kopioida tai tallentaa muilla tavoin ilman ENISAn etukäteen antamaa kirjallista lupaa tai laissa nimenomaisesti säädettyjen ehtojen tai asianomaisten oikeuksienhaltijoiden kanssa sovittujen ehtojen vastaisesti. Lähde on aina ilmoitettava. Jäljentämistä koskevat kyselyt voi lähettää julkaisussa mainittuun osoitteeseen.

© Euroopan verkko- ja tietoturvavirasto (ENISA) 2006

3 Kiitokset

ENISA haluaa kiittää kaikkia organisaatioita ja henkilöitä, jotka ovat osallistuneet tämän asiakirjan laatimiseen. Seuraavassa mainitut ansaitsevat erityisen kiitoksen:

- Henk Bronk, joka on toiminut konsulttina ja laatinut tämän asiakirjan ensimmäisen version.
- CERT/CC ja etenkin CSIRT:n kehittämisryhmä, joka on tuottanut valtaosan hyödyllisestä aineistosta ja liitteessä olevasta esimerkkiaineistosta.
- GovCERT.NL, joka on laatinut *CERT-in-a-box*-kuvauksen.
- TRANSITS-ryhmä, joka on osallistunut liitteessä olevan esimerkkiaineiston laadintaan.

- Teknisen osaston tietoturvapoliittikan yksikön työntekijät, jotka ovat osallistuneet luvun 6.6 laadintaan.
- Ne lukemattomat henkilöt, jotka ovat osallistuneet tämän asiakirjan tarkastamiseen.

4 Johdanto

Viestintäverkoista ja tietojärjestelmistä on tullut taloudellisen ja yhteiskunnallisen kehityksen olennainen tekijä. Tietojenkäsittelystä ja verkottamisesta on tulossa kaikkialla läsnä oleva hyödyke sähkön ja vesivarojen tapaan.

Viestintäverkkojen ja tietojärjestelmien turvallisuudesta ja erityisesti niiden saatavuudesta on siten tulossa yhä tärkeämpi kysymys yhteiskunnassa. Tämä johtuu paljolti siitä, että keskeisissä tietojärjestelmissä saattaa järjestelmän monimutkaisuuden, onnettomuuksien, virheiden ja iskujen takia esiintyä ongelmia, jotka voivat vaikuttaa Euroopan unionin kansalaisten hyvinvoinnin kannalta keskeisten palvelujen fyysisiin infrastruktuureihin.

Euroopan verkko- ja tietoturvavirasto (ENISA) perustettiin 10. maaliskuuta 2004.¹ Sen tärkeimpänä tavoitteena on edistää korkeatasoista verkko- ja tietoturvaa yhteisössä ja kehittää kansalaisia, kuluttajia, yrityksiä ja julkisen sektorin järjestöjä hyödyttävä verkko- ja tietoturvakulttuuri, ja siten edistää sisämarkkinoiden moitteetonta toimintaa.

Muutamat eurooppalaiset tietoturvayhteisöt, kuten CERT/CSIRT-ryhmät, väärinkäytöksiä käsittelevät ryhmät (Abuse Team) ja WARPs-ryhmät (Warning, Advice Reporting Points), ovat jo vuosien ajan tehneet yhteistyötä Internetin turvallisuuden parantamiseksi. ENISA aikoo tukea näitä yhteisöjä niiden toiminnassa antamalla tietoa toimenpiteistä, joilla voidaan varmistaa palvelujen laadun asianmukainen taso. Lisäksi ENISA aikoo lisätä valmiuksiaan neuvoa EU:n jäsenvaltioita ja EU:n elimiä asianmukaisten tietoturvapalvelujen tarjoamiseksi tietyille tietotekniikan käyttäjäryhmille. Siksi tämä uusi työryhmä aikoo tarkastella vuonna 2005 perustetun tilapäisen työryhmän "CERT Cooperation and Support" tulosten pohjalta kysymyksiä, jotka koskevat tietyille käyttäjille (käyttäjälukille tai käyttäjäryhmille) tarjottavia riittäviä tietoturvapalveluja ("CERT-palvelut").

ENISA on mukana tukemassa uusien CSIRT-ryhmien perustamista julkaisemalla tämän kertomuksen "Vaiheittainen lähestymistapa *CSIRT-tietoturvaryhmän perustamiseen ja täydentävä tarkistuslista*", josta on apua CSIRT-ryhmää perustettaessa.

¹ Euroopan verkko- ja tietoturvaviraston perustamisesta 10 päivänä maaliskuuta 2004 annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 460/2004. "Yhteisön virasto" on EU:n perustama elin, jonka vastuulla on toteuttaa erityisiä teknisiä, tieteellisiä tai hallinnollisia tehtäviä yhteisön politiikan alalla ("ensimmäinen pilari").

Kohderyhmä

Tämä kertomus on tarkoitettu ensisijaisesti valtion laitoksille ja muille laitoksille, jotka päättävät perustaa CSIRT-tietoturvaryhmän suojellakseen omaa tai sidosryhmiensä tietotekniikkainfrastruktuuria.

Asiakirjan käyttö

Asiakirjassa annetaan tietoa siitä, mikä CSIRT on, mitä palveluja se voi tarjota ja mitkä ovat välttämättömät vaiheet sen toiminnan käynnistämiseksi. Lukijalle on tarkoitus antaa hyvä ja käytännönläheinen yleiskuva CSIRT-ryhmän perustamisen menetelmistä, rakenteesta ja sisällöstä.

Luku 4 ”Johdanto”

Johdanto tähän kertomukseen

Luku 5 ”CSIRT-ryhmän suunnittelua ja perustamista koskeva yleisstrategia”

Ensimmäisessä kohdassa esitetään CSIRT-ryhmän kuvaus. Siinä annetaan myös tietoa siitä, millaisissa eri ympäristöissä CSIRT-ryhmät voivat toimia, ja siitä, minkälaisia palveluja ne voivat tarjota.

Luku 6 ”Liiketoimintasuunnitelman laatiminen”

Tässä luvussa kuvataan liikkeenjohdon lähestymistapaa perustamismenettelyssä.

Luku 7 ”Liiketoimintasuunnitelman edistäminen”

Tässä luvussa käsitellään liiketoimintaan ja rahoitukseen liittyviä kysymyksiä.

Luku 8 ”Esimerkkejä toiminnallisista ja teknisistä menettelyistä”

Tässä luvussa tarkastellaan tiedonhankintaa ja tietoturvatiedotteen laatimista näiden tietojen pohjalta. Lisäksi tässä luvussa kuvataan työnkulkua tietoturvaloukkausten käsittelyn yhteydessä.

Luku 9 ”CSIRT-koulutus”

Tässä luvussa esitetään yhteenveto saatavana olevasta CSIRT-koulutuksesta. Liitteessä on havainnollistavaa esimerkkiaineistoa.

Luku 10 ”Harjoitus: tietoturvatiedotteen laatiminen”

Tämä luku sisältää harjoituksen, joka liittyy erään CSIRT:n peruspalvelun (tai keskeisen palvelun) tuottamiseen, toisin sanoen tietoturvatiedotteen laatimiseen.

Luku 12 ”Hankesuunnitelman kuvaus”

Tässä luvussa käsitellään oppaassa esitettyä täydentävää hankesuunnitelmaa (tarkistuslistaa). Suunnitelman on tarkoitus olla yksinkertainen väline oppaan panemiseksi täytäntöön.

Asiakirjan rakenne

Paremmän yleiskuvan saamiseksi jokaisen luvun alussa esitetään yhteenveto CSIRT-ryhmän perustamismenettelyssä toistaiseksi toteutetuista toimista. Yhteenvedot on laatikoitu seuraavaan tapaan:

Ensimmäinen vaihe on nyt toteutettu.

Jokainen luku sisältää käytännön esimerkin tarkasteltavista vaiheista. Tässä asiakirjassa "kuvitteellisella CSIRT-ryhmällä" tarkoitetaan keskisuuren yrityksen tai laitoksen pientä itsenäistä CSIRT-ryhmää. Yhteenveto esitetään liitteessä.

Kuvitteellinen CSIRT

5 CSIRT-ryhmän suunnittelun ja perustamisen yleinen strategia

Jotta CSIRT-ryhmän perustaminen saadaan onnistuneesti alkuun, on tärkeää luoda selkeä kuva niistä mahdollisista palveluista, joita ryhmä voi tarjota asiakkailleen. Näistä käytetään CSIRT-ympäristössä englanninkielistä termiä "constituents" (asiakkaat). On ymmärrettävä, mitkä ovat asiakkaiden tarpeet, jotta voidaan tarjota riittävän ajantasaisia ja laadultaan oikean tasoisia palveluja.

Mikä on CSIRT?

CSIRT:llä tarkoitetaan tietoturvaloukkauksia käsittelevää ryhmää (Computer Security Incident Response Team). Käsitettä CSIRT käytetään ensisijaisessa Euroopassa tarkoittamaan suojattua käsitettä CERT, joka on Yhdysvalloissa CERT Coordination Center -keskuksen (CERT/CC) rekisteröimä käsite.

Samankaltaisista ryhmistä käytetään erilaisia lyhenteitä:

- CERT tai 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)

Maailmanlaajuisessa tietotekniikkainfrastruktuurissa ensimmäinen matona leviävä merkittävä haittaohjelma havaittiin 1980-luvun lopussa. Matoa kutsuttiin nimellä Morris², ja se levisi nopeasti ja tehokkaasti tartuttaen suuren määrän tietotekniikkajärjestelmiä eri puolella maailmaa.

Tämä tapaus herätti ihmiset huomaamaan, että on välttämätöntä varmistaa järjestelmän hallintoijien ja tietotekniikkapäälliköiden välinen yhteistyö ja koordinointi tällaisten tapausten ratkaisemiseksi. Koska aika oli eräs kriittinen tekijä, tietoturvaongelmien käsittelyssä oli omaksuttava entistä organisoidumpi ja jäsennellympi lähestymistapa. Muutama päivä Morris-madon aiheuttaman uhan jälkeen DARPA (Defence Advanced Research Projects Agency) perusti ensimmäisen CSIRT-ryhmän, CERT Coordination Center -keskuksen (CERT/CC³), joka sijaitsee Carnegie Mellonin yliopistossa Pittsburghissa Pennsylvaniassa.

Tämä malli omaksuttiin pian myös Euroopassa, ja vuonna 1992 hollantilainen palveluntarjoaja ja yliopistoverkko SURFnet perusti ensimmäisen eurooppalaisen CSIRT-ryhmän nimeltä SURFnet-CERT.⁴ Sen jälkeen on perustettu monia uusia tietoturvaryhmiä, ja ENISAn laatimassa CERT-toimia koskevassa luettelossa "*Inventory of CERT activities in Europe*"⁵ luetellaan yli 100 Euroopassa toimivaa tietoturvaryhmää.

² Lisätietoa Morris-madosta osoitteessa: 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/

Vuosien mittaan CERT-ryhmät ovat laajentaneet valmiuksiaan, eivätkä ne ole enää pelkästään reaktioryhmiä vaan ne tarjoavat kattavia turvapalveluja, mukaan luettuina ennalta ehkäisevät palvelut, kuten hälytykset, tietoturvatiedotteet, koulutus ja tietoturvan hallinnan palvelut. Käsitettä "CERT" alettiin pitää pian riittämättömänä. Niinpä 1990-luvun lopussa otettiin käyttöön uusi käsite "CSIRT". Tällä hetkellä näitä käsitteitä (CERT ja CSIRT) käytetään toistensa synonyymeinä, mutta CSIRT on käsitteistä tarkempi.

5.1 Käsite "**Constituency**" (asiakaskunta)

Jäljempänä käytetään (CSIRT-yhteisöissä) vakiintunutta käsitettä "asiakaskunta" ("**Constituency**") viittamaan CSIRT:n asiakkaisiin. Yksittäistä käyttäjää kutsutaan käsitteellä "asiakas" ja käyttäjäryhmää käsitteellä "asiakkaat".

5.2 CSIRT:n määritelmä

CSIRT on tietoturva-asiantuntijoiden muodostama ryhmä, jonka päätehtävänä on käsitellä tietoturvaloukkauksia. Se tarjoaa palveluja, jotka ovat välttämättömiä tietoturvaloukkausten käsittelemiseksi ja asiakkaiden toipumiseksi tietoturvaloukkausten aiheuttamista häiriöistä.

Vaarojen lieventämiseksi ja tarvittavien toimien määrän minimoimiseksi useimmat CSIRT-ryhmät tarjoavat asiakkailleen myös ennalta ehkäiseviä palveluja ja koulutuspalveluja. Ne laativat tiedotteita, jotka koskevat käytössä olevien ohjelmistojen ja laitteistojen turva-aukkoja, ja tiedottavat käyttäjille hyökkäyksistä ja viruksista, jotka hyödyntävät tällaisia turva-aukkoja. Asiakkaat voivat siten asentaa vaadittavat korjaukset ja päivitykset järjestelmiinsä nopeasti. Luvussa 5.2 "*CSIRT-ryhmän mahdolliset palvelut*" esitetään kattava luettelo mahdollisista palveluista.

5.3 CSIRT-ryhmän tarjoama hyöty

Erillinen tietoturvaryhmä auttaa organisaatiota vähentämään suurten tietoturvaloukkausten määrää ja estämään ne sekä suojaamaan sen arvokasta omaisuutta.

Muita mahdollisia hyötyjä ovat:

- tietoturvakysymysten keskitetty koordinointi organisaatiossa (Point of Contact, PoC)
- tietoturvaloukkausten keskitetty ja eriytetty käsittely ja ratkaiseminen
- asiantuntemus, jonka pohjalta käyttäjiä tuetaan ja autetaan palautumaan nopeasti tietoturvaloukkauksista
- lainopillisten kysymysten käsitteleminen ja todisteiden säilyttäminen oikeuskanteiden varalta
- tietoturva-alan kehityskulkujen seuraaminen
- asiakaskunnan kannustaminen yhteistyöhön tietoturvakysymyksissä (tietoisuuden parantaminen).

Kuvitteellinen CSIRT (vaihe 0)

Mikä on CSIRT?

Malliesimerkiksi valitaan CSIRT-ryhmä, joka tarjoaa palveluja keskikokoiselle, 200 työntekijän laitokselle. Laitoksella on oma tietotekniikkaosasto ja kaksi muuta sivutoimipistettä samassa maassa. Tietotekniikka on keskeisessä asemassa yhtiössä, sillä sitä käytetään sisäistä viestintää, tietoverkkoja ja vuorokauden ympäri tapahtuvaa (24x7) sähköistä liiketoimintaa varten. Laitoksella on oma verkko ja lisäyhteys Internetiin kahden eri Internet-palveluntarjoajan (ISP) välityksellä.

5.4 Erilaisten CSIRT-ympäristöjen kuvaus

Ensimmäinen vaihe on nyt toteutettu.

1. Mikä on CSIRT ja mitä hyötyä siitä voi olla?

>> Seuraavassa vaiheessa vastataan kysymykseen: *"Mitkä alat käyttävät CSIRT-palveluja?"*

CSIRT:n (kuten minkä tahansa yrityksen) perustamisen yhteydessä on hyvin tärkeää luoda mahdollisimman pian selkeä näkemys siitä, ketkä kuuluvat asiakaskuntaan ja minkälaisia toimintaympäristöjä varten CSIRT-palveluja kehitetään. Näitä ovat aakkosjärjestyksessä seuraavat:

- CIP/CIIP-ala
- kansallinen CSIRT
- kaupallinen ala
- korkeakouluala
- palveluntarjoajat
- pienet ja keski suuret yritykset (pk-yritykset)
- sisäinen CSIRT
- sotilasala
- valtionhallinto

CIP/CIIP-alan CSIRT-ryhmä

Painopiste

Tällä alalla toimivat CSIRT-ryhmät keskittyvät lähinnä erittäin tärkeän tiedon suojaamiseen ja/tai erittäin tärkeän tiedon ja infrastruktuurin suojaamiseen. Tällaiset erikoistuneet CSIRT-ryhmät tekevät usein tiiviistä yhteistyötä valtionhallinnon CIIP-osaston kanssa. Ne tarjoavat palveluja kaikille maan elintärkeille IT-aloille ja suojelevat näin maan kansalaisia.

Asiakkaat

Valtio, erittäin tärkeän tiedon IT-yritykset, kansalaiset

Kansallinen CSIRT

Painopiste

Kansallinen CSIRT-ryhmä on maan tietoturvakysymyksistä vastaava yhteystaho. Joissakin tapauksissa valtion CSIRT toimii myös kansallisena yhteispisteenä (kuten UNIRAS Yhdistyneessä kuningaskunnassa).

Asiakkaat

Tällaisella CSIRT-ryhmällä ei ole yleensä suoria asiakkaita, sillä kansallinen CSIRT-ryhmä toimii ainoastaan välittäjänä koko maassa.

Kaupallisen alan CSIRT-ryhmät*Painopiste*

Kaupallisen alan CSIRT-ryhmät tarjoavat asiakkailleen kaupallisia CSIRT-palveluja. Jos kyse on Internet-palveluntarjoajasta, CSIRT-ryhmä tarjoaa loppukäyttäjille (Dial-in, ADSL) useimmiten palveluja tietojen väärinkäytön estämiseksi ja CSIRT-palveluja asiakkaiden ammattikäyttöön.

Asiakkaat

Kaupalliset CSIRT-ryhmät tuottavat palveluja asiakkailleen yleensä maksua vastaan.

Korkeakoulualan CSIRT-ryhmät*Painopiste*

Korkeakoulualalla toimivat CSIRT-ryhmät tarjoavat CSIRT-palveluja korkeakouluille ja oppilaitoksille, kuten yliopistoille tai tutkimuslaitoksille, ja kampuksen Internet-ympäristöille.

Asiakkaat

Tällaisen CSIRT-ryhmän asiakkaita ovat tavallisesti yliopistojen henkilökunta ja opiskelijat.

Pienten ja keskisuurten yritysten CSIRT-ryhmät*Painopiste*

CSIRT-ryhmä, jolla on oma organisaatio ja joka tarjoaa palvelujaan omalle toimialalleen tai vastaaville käyttäjäryhmille.

Asiakkaat

Tällaisten CSIRT-ryhmien asiakkaita voivat olla pk-yritykset ja niiden henkilöstö tai erityiset eturyhmät, kuten kaupunki- ja kuntaliitot.

Palveluntarjoajien CSIRT-ryhmät*Painopiste*

Palveluntarjoajan CSIRT-ryhmän painopiste on palveluntarjoajan tuotteille annettavassa tuessa. Ryhmän tavoitteena on yleensä kehittää ja tarjota ratkaisuja heikkojen kohtien poistamiseksi ja vikojen mahdollisten haitallisten vaikutusten lieventämiseksi.

Asiakkaat

Tuoteomistajat

Sisäiset CSIRT-ryhmät*Painopiste*

Sisäiset CSIRT-ryhmät tarjoavat palveluja ainoastaan toimeksiantajaorganisaatioille. Käsitteellä kuvataan pikemminkin toimintatapaa kuin toiminta-alaa. Monilla televiestintäyrityksillä ja esimerkiksi pankeilla on omat sisäiset CSIRT-ryhmänsä. Ne eivät yleensä pidä yllä yleisölle avointa verkkoa.

Asiakkaat

Toimeksiantajaorganisaation sisäinen henkilöstö ja IT-osasto.

Sotilasalan CSIRT-ryhmät**Painopiste**

Sotilasalan CSIRT-ryhmät tarjoavat palveluja sotilasorganisaatioille, jotka ovat vastuussa puolustustarkoitukseen käytettävästä tietotekniikan infrastruktuurista.

Asiakkaat

Sotilasorganisaatioiden tai niihin läheisesti liittyvien elinten, kuten puolustusministeriön, henkilöstö

Valtionhallinnon CSIRT-ryhmät**Painopiste**

Valtionhallinnon CSIRT-ryhmät tarjoavat palveluja valtion virastoille ja joissakin maissa kansalaisille.

Asiakkaat

Valtio ja valtion virastot; joissakin maissa palveluja tarjotaan myös kansalaisille (esimerkiksi Belgiassa, Unkarissa, Alankomaissa, Yhdistyneessä kuningaskunnassa tai Saksassa).

Kuten kansallisia CSIRT-ryhmiä koskevassa kohdassa todetaan, ryhmä voi tarjota palveluja useammalle kuin yhdelle ryhmälle. Tällä on vaikutusta esimerkiksi asiakaskunnan ja sen tarpeiden analyysin kannalta.

Kuvitteellinen CSIRT (vaihe 1)**Aloitusvaihe**

Aloitusvaiheessa uusi CSIRT-ryhmä määritetään organisaation sisäiseksi tietoturvaryhmäksi, ja se tarjoaa palveluja toimeksiantajaorganisaatiolle, paikalliselle IT-osastolle ja henkilöstölle. Lisäksi sillä on avustava ja koordinoiva tehtävä yksittäisten toimistojen välillä tietoturvaloukkausten käsittelyssä.

CSIRT-ryhmän mahdolliset palvelut

Kaksi ensimmäistä vaihetta on nyt käyty läpi:

1. Sen ymmärtäminen, mikä on CSIRT ja mitä hyötyä siitä voi olla.
2. Mille toimialalle uusi ryhmä tarjoaa palveluja?

>> Seuraavassa vaiheessa vastataan kysymykseen: *"Mitä palveluja asiakkaille tarjotaan?"*

CSIRT-ryhmä voi tuottaa monenlaisia palveluja, mutta toistaiseksi yksikään nykyisistä CSIRT-ryhmistä ei tarjoa kaikkia näistä palveluista. Siksi oikeiden palvelujen valinta on

hyvin tärkeä päätös. Jäljempänä esitetään lyhyt yleiskuva kaikista tunnetuista CSIRT-palveluista, jotka on määritetty CERT/CC:n julkaisemassa käsikirjassa (Handbook for CSIRTs)⁶.

<u>Reaktiiviset palvelut</u>	<u>Proaktiiviset palvelut</u>	<u>Artefaktien käsittely</u>
• <u>Hälytykset ja varoitukset</u> • <u>Tietoturvaloukkausten käsittely</u> • <u>Tietoturvaloukkausten analysointi</u> • <u>Tietoturvaloukkausten torjunnan tukeminen</u> • <u>Tietoturvaloukkausten torjunnan koordinoiti</u> • <u>Tietoturvaloukkausten torjunta itse paikalla</u> • <u>Heikkojen kohtien käsittely</u> • <u>Heikkojen kohtien analysointi</u> • <u>Haavoittuvuuden torjunta</u> • <u>Haavoittuvuuden torjunnan koordinoiti</u>	• <u>Tiedotteet</u> • <u>Teknologian seuranta</u> • <u>Tietoturvatarkastukset tai -arvioinnit</u> • <u>Tietoturvan määrittäminen ja ylläpitäminen</u> • <u>Tunkeutumisen havaitseminen</u> • <u>Tietoturvaan liittyvien tietojen jakaminen</u>	• <u>Artefaktien analysointi</u> • <u>Artefaktien torjunta</u> • <u>Artefaktien torjunnan koordinoiti</u>
		<u>Tietoturvan laadunhallinta</u>
		• <u>Riskianalyysi</u> • <u>Liiketoiminnan jatkuvuus ja vahingoista toipuminen</u> • <u>Tietoturvanneuvonta</u> • <u>Tietoisuuden lisääminen</u> • <u>Koulutus/opetus</u> • <u>Tuotteen arviointi tai sertifiointi</u>

Kuva 1: CERT/CC:n CSIRT-palveluluettelo⁷

Keskeiset palvelut (merkitty lihavoituna): reaktiivisten ja proaktiivisten palvelujen välillä tehdään ero. Proaktiivisilla palveluilla pyritään torjumaan tietoturvaloukkaukset lisäämällä tietoisuutta ja tarjoamalla koulutusta, kun taas reaktiiviset palvelut liittyvät tietoturvaloukkausten käsittelyyn ja niistä aiheutuvien vahinkojen lieventämiseen.

Artefaktien käsittely sisältää järjestelmän sellaisen tiedoston tai kohteen analyysin, johon voi liittyä haitallisia tapahtumia. Tällaisia ovat virusten, matojen, komentosarjojen, troijanhevosten ja muiden vastaavien jäännökset. Lisäksi se kattaa saadun tiedon käsittelyn ja toimittamisen palveluntarjoajille ja muille asianosaisille tahoille, jotta estetään haittaohjelmien leviäminen edelleen ja lievennetään riskejä.

Tietoturvan hallinta ja laadunhallinta ovat palveluja, joilla on pitkän aikavälin tavoitteet. Tällaisia ovat esimerkiksi konsultointi- ja koulutustoimet.

Katso CSIRT-palvelujen yksityiskohtainen kuvaus liitteestä.

Oikeiden palvelujen valinta asiakaskunnalle on tärkeä vaihe, ja sitä tarkastellaan lähemmin luvussa 6.1 "Rahoitusmallin määrittäminen".

⁶ CERT/CC CSIRT:n käsikirja: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

⁷ CERT/CC:n CSIRT-palveluluettelo: <http://www.cert.org/csirts/services.html>

Useimmat CSIRT-ryhmät jakavat aluksi asiakaskunnalleen hälytyksiä ja varoituksia, laativat tiedotteita ja käsittelevät tietoturvaloukkauksia. Tällaisten keskeisten palvelujen avulla saadaan yleensä hyvin näkyvyyttä ja huomioarvoa asiakaskunnan keskuudessa, ja ne tuovat yleensä todellista lisäarvoa.

Hyvä käytäntö on aloittaa niin kutsuttujen pilottiasiakkaiden muodostamasta pienestä ryhmästä, toimittaa keskeisiä palveluja pilottiajanjakson ajan ja pyytää myöhemmin palautetta.

Asiasta kiinnostuneet pilottikäyttäjät antavat yleensä rakentavaa palautetta ja auttavat kehittämään räätälöityjä palveluja.

Kuvitteellinen CSIRT-ryhmä (vaihe 2)

Oikeiden palvelujen valinta

Alkuvaiheessa päätetään, että uusi CSIRT-ryhmä keskittyy pääasiassa muutamien keskeisten palvelujen tarjoamiseen työntekijöille.

Päätetään, että pilottivaiheen jälkeen voidaan pohtia palveluvalikoiman laajentamista ja että siihen voidaan lisätä ”tietoturvan hallinnan palveluja”. Tällaisen päätöksen tulee perustua pilottiasiakkailta saatuun palautteeseen, ja se tehdään tiiviissä yhteistyössä laadunvarmistusosaston kanssa.

Asiakaskunnan analysointi ja toimenkuvan määrittäminen

Ensimmäiset kolme vaihetta on nyt toteutettu:

1. Mikä on CSIRT ja mitä hyötyä siitä on?
2. Mille toimialalle uusi ryhmä tarjoaa palveluja?
3. Mitä palveluja CSIRT-ryhmä voi tarjota asiakaskunnalleen?

>> Seuraavassa vaiheessa vastataan kysymykseen: *”Minkälaista lähestymistapaa sovelletaan CSIRT-ryhmän perustamisessa?”*

Seuraavassa vaiheessa tarkastellaan yksityiskohtaisemmin asiakaskuntaa ja pyritään valitsemaan oikeat viestintäkanavat:

- määritetään, millä tavoin viestitään asiakaskunnalle
- määritetään toimenkuva
- laaditaan realistinen toteutus-/hankesuunnitelma
- määritetään CSIRT-palvelut
- määritetään organisaatorakenne
- määritetään tietoturvapolitiikka
- palkataan oikeanlaista henkilöstöä
- hyödynnetään omaa CSIRT-toimistoa

- pyritään tekemään yhteistyötä muiden CSIRT-ryhmien ja mahdollisten kansallisten aloitteiden kanssa

Näitä vaiheita kuvataan yksityiskohtaisemmin seuraavissa kohdissa, ja ne voidaan sisällyttää liiketoiminta- ja hankesuunnitelmaan.

5.1 Viestintäkanavat asiakaskunnalle tiedottamiseksi

Kuten edellä on todettu, on hyvin tärkeää määrittää asiakaskunnan tarpeet ja oma viestintästrategia, johon sisältyvät kaikkein asianmukaisimmat viestintäkanavat asiakaskunnalle tiedottamiseksi.

Johtamisteoriassa tunnetaan useita mahdollisia lähestymistapoja, joita voidaan soveltaa kohderyhmän analysoinnissa. Tässä asiakirjassa tarkastelemme kahta tällaista lähestymistapaa: SWOT- ja PEST-analyysia.

SWOT-analyysi

SWOT-analyysi (lyhenne englanninkielisistä sanoista **S**trengths, **W**eaknesses, **O**pportunities ja **T**hreats) on strateginen suunnitteluväline, jolla arvioidaan hankkeeseen tai yritystoimintaan tai mihin tahansa muuhun päätöstä vaativaan tilanteeseen liittyviä vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia. Menetelmän on kehittänyt Albert Humphrey, joka johti Stanfordin yliopistossa 1960- ja 1970-luvulla erästä tutkimushanketta Fortune 500 -yrityksiä koskevien tietojen pohjalta.⁸

Vahvuudet	Heikkoudet
Mahdollisuudet	Uhat

Kuva 2: SWOT-analyysi

⁸ SWOT-analyysi Wikipediassa: http://en.wikipedia.org/wiki/SWOT_analysis

PEST-analyysi

PEST-analyysi (lyhenne englanninkielisistä sanoista **P**olitical, **E**conomic, **S**ocio-cultural ja **T**echnological) on toinen tärkeä ja laajasti käytetty väline, jolla analysoidaan asiakaskuntaa ja jonka avulla pyritään ymmärtämään CSIRT:n poliittista, taloudellista, sosiaalista ja kulttuurista sekä teknologista toimintaympäristöä. Välineen avulla voidaan selvittää, vastaako suunnittelu edelleen toimintaympäristön olosuhteita, ja autetaan välttämään vääriin olettamuksiin perustuvia toimia.

Poliittiset tekijät • Ekologiset kysymykset / ympäristökysymykset • Voimassa oleva lainsäädäntö kotimaassa • Tuleva lainsäädäntö • Eurooppalainen/kansainvälinen lainsäädäntö • Sääntelyelimet ja -menettelyt • Hallituksen politiikka • Hallituksen toimikausi ja vaihtuminen • Kauppapolitiikka • Rahoitus, apurahat ja aloitteet • Etu-/painostusryhmät kotimaassa • Kansainväliset painostusryhmät	Taloudelliset tekijät • Kotimaan taloudellinen tilanne • Kotimaan taloussuhdanteet • Taloussuhdanteet ja talouden kehittyminen ulkomailla • Yleiset vero-oikeudelliset kysymykset • Tuotteiden/palvelujen verotus • Kausi-/sääkohtaiset kysymykset • Markkina- ja suhdannesykli • Alakohtaiset tekijät • Markkinointikanavat ja jakelusuuntaukset • Asiakkaisiin/loppukäyttäjiin liittyvät liikkeellepanevat tekijät • Korkoasteet ja vaihtokurssit
Sosiaaliset tekijät • Elämäntapatrendit • Väestötiede • Kuluttajien asenteet ja mielipiteet • Tiedotusvälineiden näkemykset • Sosiaalisiin tekijöihin vaikuttavat lakimuutokset • Merkkiin, yritykseen ja teknologiaan liittyvä imago • Kuluttajien ostokäyttäytyminen • Muoti ja roolimallit • Merkittävät tapahtumat ja vaikutukset • Ostomahdollisuudet ja -suuntaukset • Etniset/uskonnolliset tekijät • Mainonta ja julkisuus	Teknologiset tekijät • Kilpailevan tekniikan kehittyminen • Tutkimuksen rahoittaminen • Asiaan liittyvä/riippuvainen teknologia • Korvaava teknologia/korvaavat ratkaisut • Teknologian kehittyneisyys • Tuotannon kehittyneisyys ja kapasiteetti • Tiedottaminen ja viestintä • Kuluttajien ostomenetelmät/-teknologia • Teknologiaa koskeva lainsäädäntö • Innovaatiopotentiali • Teknologian saatavuus, lupajärjestelmä, patentit • Aineetonta omaisuutta koskevat kysymykset

Kuva 3: Pest-analyysimalli

Yksityiskohtainen kuvaus PEST-analyysistä esitetään Wikipediassa.⁹

Molemmilla välineillä saadaan kattava ja jäsenneilty yleiskuva asiakaskunnan tarpeista. Tuloksilla täydennetään liiketoimintaehdotuksia ja helpotetaan näin rahoituksen saamista CSIRT:n perustamiseksi.

Viestintäkeinot

Eräs analyysiin sisällytettävä tärkeä aihe on mahdolliset viestintä- ja tiedotusmenetelmät (Viestintä asiakaskunnan kanssa).

⁹ PEST-analyysi Wikipediassa: http://en.wikipedia.org/wiki/PEST_analysis

Mahdollisuuksien mukaan olisi harkittava säännöllisiä vierailuja asiakaskunnan luo. On osoitettu, että tällaisilla henkilökohtaisilla tapaamisilla helpotetaan yhteistyötä. Jos molemmat osapuolet ovat halukkaita yhteistyöhön, tällaiset tapaamiset johtavat avoimempaan suhteeseen.

Yleensä CSIRT-ryhmät käyttävät useita viestintäkeinoja. Seuraavat keinot ovat osoittautuneet hyödyllisiksi käytännössä, ja ne ovat pohtimisen arvoisia:

- julkinen verkkosivusto
- rajattu jäsensivusto
- sähköiset lomakkeet tietoturvaloukkauksista raportoimiseksi
- postituslistat
- henkilökohtainen sähköposti
- puhelin/faksi
- tekstiviestit
- paperimuodossa hoidettava kirjeenvaihto
- kuukausi- tai vuosikertomukset

Sen lisäksi että tietoturvaloukkausten käsittelyn helpottamiseksi käytetään sähköpostia, Internet-lomakkeita, puhelinta tai faksia (tietoturvaloukkauksia koskevien raporttien vastaanottamiseen asiakaskunnalta, toimien koordinoimiseksi muiden ryhmien kanssa tai palautteen ja tuen antamiseksi) useimmat CSIRT-ryhmät julkaisevat tietoturvatiedotteita julkisilla verkkosivuilla ja postituslistojen välityksellä.

! Tiedon jakamisessa olisi käytettävä mahdollisuuksien mukaan suojattuja menetelmiä. Sähköpostit voidaan allekirjoittaa esimerkiksi digitaalisesti käyttämällä julkisen avaimen salausmenetelmää (PGP), ja tietoturvaloukkauksia koskevat luottamukselliset tiedot olisi aina lähetettävä salattuina.

Ks. lisätietoa luvusta 8.5 ”Käytettävissä olevat CSIRT-työkalut”. Ks. myös RFC2350:n luku 2.3.¹⁰

Kuvitteellinen CSIRT (vaihe 3a)

Asiakaskunnan ja asianmukaisten viestintäkeinojen analysointi

Liikkeenjohdon ja asiakaskunnan avainhenkilöiden kanssa järjestetyssä ideariihessä tuotetaan riittävästi tietoa SWOT-analyysia varten. Sen perusteella voidaan päätellä, että seuraavat keskeiset palvelut ovat välttämättömiä:

- hälytykset ja varoitukset
- tietoturvaloukkausten käsittely (analyysi, tuen antaminen ja torjunnan koordinointi)
- tiedotteet

On varmistettava, että tiedottaminen on hyvin organisoitua, jotta saavutetaan mahdollisimman suuri osa asiakaskunnasta. Näin ollen päätetään, että hälytykset, varoitukset ja tiedotteet julkaistaan tietoturvatiedotteina erityisellä verkkosivulla ja

¹⁰ <http://www.ietf.org/rfc/rfc2350.txt>

jaetaan käyttämällä postituslistaa. CSIRT käyttää tietoturvaloukkauksia koskevien raporttien vastaanottamiseen sähköpostia, puhelinta ja faksia. Seuraavassa vaiheessa on tarkoitus suunnitella yhtenäistä Internet-lomaketta.

Ks. SWOT-analyysia koskeva malliesimerkki jäljempänä.

Vahvuudet - Yrityksellä on jo jonkin verran tietämystä asiasta - Yritys kannattaa suunnitelmaa ja on halukas yhteistyöhön - Hallintoneuvoston antama tuki ja rahoitus	Heikkoudet - Vähän viestintää eri osastojen ja sivuliikkeiden välillä - Ei koordinointia tietoturvaloukkausten alalla - Paljon pieniä osastoja
Mahdollisuudet - Heikkoihin kohtiin liittyvien jäsentymättömien tietojen suuri määrä - Suuri koordinointitarve - Tietoturvaloukkauksista aiheutuvat vahingot vähentyvät - Useita avoimia tietoturvakysymyksiä - Henkilöstön kouluttaminen tietoturvan alalla	Uhat - Vain vähän varoja käytettävissä - Vähän henkilöstöä - Suuret odotukset - Kulttuuri

Kuva 4: Esimerkki SWOT-analyysista

5..2 Toimenkuva

Kun asiakaskunnan CSIRT-palveluja koskevat tarpeet ja toiveet on analysoitu, seuraavassa vaiheessa on määritettävä toimenkuva.

Toimenkuvaa koskevassa määritelmässä esitetään yrityksen perustehtävä yhteisössä sen asiakaskunnalleen tarjoamien tuotteiden ja palvelujen osalta. Siinä esitetään selkeästi, mikä on uuden CSIRT:n tarkoitus ja tehtävä.

Käytännössä on suositeltavaa määrittää toimenkuva lyhyesti muttei kuitenkaan liian suppeasti, sillä yleensä se pysyy muuttumattomana muutaman vuoden ajan.

Jäljempänä esitetään muutamia esimerkkejä toiminnassa olevien CSIRT-ryhmien toimenkuvista:

"<CSIRT:n nimi> antaa tietoa ja tukea <asiakkailleen (määritä asiakkaat)> proaktiivisten toimenpiteiden toteuttamisessa tietoturvaloukkauksiin liittyvien uhkien vähentämiseksi ja tällaisten mahdollisesti ilmenevien tietoturvaloukkausten ratkaisemiseksi."

"Antaa tukea <asiakkailleen> IT-alaan liittyvien tietoturvaloukkausten torjumisessa ja käsittelyssä"¹¹

Toimenkuvan määrittäminen on hyvin tärkeä ja välttämätön vaihe. Asiakirjan *RFC2350*¹² luvussa 2.1 esitetään yksityiskohtaisempi kuvaus siitä, minkälaista tietoa CSIRT:n olisi julkaistava.

Kuvitteellinen CSIRT (vaihe 3b)

Kuvitteellisen CSIRT:n johdon on määriteltävä toimenkuva seuraavasti:

"Kuvitteellinen CSIRT antaa tietoa ja tukea toimeksiantajansa henkilöstölle vähentääkseen tietoturvaloukkauksiin liittyviä uhkia ja ratkaistakseen tällaiset mahdolliset tapahtumat."

Kuvitteellinen CSIRT selventää näin, että se on yrityksen sisäinen tietoturvaryhmä ja että sen keskeisenä tehtävänä on käsitellä IT-alan tietoturvakysymyksiä.

¹¹ Govcert.nl:n toimenkuvan määrittäminen: <http://www.govcert.nl>

¹² <http://www.ietf.org/rfc/rfc2350.txt>

6 Liiketoimintasuunnitelman laatiminen

Tähän mennessä on toteutettu seuraavat vaiheet:

1. Mikä on CSIRT ja mitä hyötyä siitä on?
2. Mille toimialalle uusi ryhmä tarjoaa palvelujaan?
3. Mitä palveluja CSIRT-ryhmä voi tarjota asiakaskunnalleen?
4. Toimintaympäristön ja asiakkaiden arviointi
5. Toimenkuvan määrittäminen

>> Seuraavassa vaiheessa määritetään liiketoimintasuunnitelma

Analyysin tulosten perusteella saadaan hyvä yleiskuva asiakaskunnan tarpeista ja (oletetuista) heikkouksista, ja ne otetaan huomioon seuraavassa vaiheessa.

Rahoitusmallin määrittäminen

Analyysin jälkeen valitaan muutama keskeinen palvelu, joilla toiminta käynnistetään. Seuraavassa vaiheessa on pohdittava rahoitusmallia, toisin sanoen sitä, mitkä palveluparametrit ovat soveltuvia ja rahoitettavissa.

Ihannetapauksessa rahoitus mukautettaisiin vastaamaan asiakaskunnan tarpeita, mutta todellisuudessa tarjottava palveluvalikoima on kuitenkin mukautettava vastaamaan tiettyä budjettia. Siksi onkin realistisempaa aloittaa rahoituskysymysten suunnittelusta.

6..1 Kustannusmalli

Kustannuksiin vaikuttavat kaksi päätekijää ovat palveluaikojen ja palkattavan henkilöstön määrän (ja laadun) määrittäminen. Onko tietoturvaloukkausten käsittely ja tekninen tuki taattava vuorokauden ympäri (24x7), vai tarjotaanko tällaisia palveluja ainoastaan tavanomaisina toimistoaikoina?

Toivottujen palveluaikojen ja toimistolaitteiden mukaan (onko esim. etättyö mahdollista) voi olla hyödyllistä käyttää joko päivystysvuorolistaa tai säännöllistä työvuorolistaa.

Eräs mahdollinen toimintatapa on tuottaa sekä proaktiivisia että reaktiivisia palveluja toimistoaikoina. Toimistoaikojen ulkopuolella päivystävä henkilöstö tarjoaisi vain tiettyjä palveluja, esimerkiksi hätätapauksissa ja poikkeuksellisissa tilanteissa.

Toinen mahdollisuus on pohtia kansainvälistä yhteistyötä muiden CSIRT-ryhmien kanssa. On jo olemassa esimerkkejä "Following the Sun" -periaatteella toimivasta yhteistyöstä. Esimerkiksi eurooppalaisten ja yhdysvaltalaisen tietoturvaryhmien välinen yhteistyö on osoittautunut hyödylliseksi, ja se on hyvä keino jakaa kapasiteettia vastavuoroisesti. Esimerkiksi Sun Microsystems, jolla on useita sivuliikkeitä eri aikavyöhykkeillä eri puolilla maailmaa (mutta jotka ovat saman CSIRT-ryhmän jäseniä), tarjoaa ympärivuorokautisia (24x7) palveluja vuorottelemalla jatkuvasti eri puolilla

maailmaa toimivien ryhmien kesken. Näin vähennetään kustannuksia, sillä ryhmät toimivat aina ainoastaan tavanomaisina toimistoaikoina, ja ne tarjoavat palveluja myös ”nukkuvalle osalle” maailmaa.

Hyvä käytäntö on analysoida ympärivuorokautisten (24x7) palvelujen tarvetta perusteellisesti asiakaskunnan kanssa. Yöaikana annetuista hälytyksistä ja varoituksista ei ole hyötyä, jos vastaanottaja lukee ne vasta seuraavana aamuna. ”Tarvittavien palvelujen” ja ”toivottujen palvelujen” välillä on hienoinen ero, mutta etenkin työajoilla on valtava vaikutus henkilöstön määrään ja tarvittaviin laitteistoihin, ja niillä on siten valtava merkitys kustannusmallin kannalta.

6..2 Tulomalli

Kun kustannukset ovat tiedossa, seuraavassa vaiheessa on syytä pohtia mahdollisia tulomalleja eli sitä, miten suunnitellut palvelut voidaan rahoittaa. Jäljempänä esitetään muutamia vaihtoehtoisia malleja arvioitavaksi:

Resurssien hyödyntäminen

On aina hyödyllistä arvioida yrityksen muissa osissa jo saatavilla olevia resursseja. Onko yrityksellä jo sopivaa henkilöstöä (esimerkiksi nykyisessä IT-osastossa), jolla on tarvittavat taustatiedot ja asiantuntemusta? Ehkä yritysjohto voi tehdä tarvittavat järjestelyt, jotta tätä henkilöstöä voidaan käyttää CSIRT-ryhmän tarpeisiin alkuvaiheessa, tai ehkä se voi antaa väliaikaista tukea CSIRT-ryhmälle.

Jäsenmaksu

Toinen mahdollisuus on myydä palveluja asiakaskunnalle vuosi- tai neljännesvuosimaksua vastaan. Lisäpalveluista, kuten konsultointipalvelusta tai tietoturvatarkastuksista, voitaisiin maksaa käytön mukaan.

Toinen mahdollinen menettelytapa on tarjota (yrityksen sisäiselle) asiakaskunnalle palveluja maksutta mutta veloittaa ulkoisille asiakkaille tuotettavista palveluista. Eräs vaihtoehto on julkaista tiedotteita ja tiedonantoja julkisella verkkosivulla ja ylläpitää ainoastaan jäsenille tarkoitettuja sivuja, joilla annetaan yksityiskohtaisempaa ja räätälöidymää tietoa.

Käytännössä on osoitettu, että etenkin käynnistysvaiheessa yksittäisiä CSIRT-palveluja koskevilla tilauksilla (Subscription per service) saadaan vain osa tarvittavista rahoitusvaroista. Esimerkiksi ryhmästä ja laitteistoista on maksettava kiinteitä maksuja etukäteen. On vaikeaa rahoittaa tällaisia kustannuksia myymällä CSIRT-palveluja, ja se edellyttää hyvin yksityiskohtaista rahoitusanalyysia kannattavuuskynnyksen määrittämiseksi.

Valtiontuki

Eräs harkinnan arvoinen vaihtoehto on anoa hankkeelle valtion tai jonkin valtioelimen myöntämää tukea, sillä nykyään monissa maissa on saatavana rahoitusta IT-alan tietoturvahankkeita varten. Yhteydenotto sisäministeriöön voi olla hyvä keino päästä alkuun.

Eri tulomalleja voidaan tietenkin yhdistää.

Organisaatorakenteen määrittäminen

CSIRT:n asianmukaisen organisaatorakenteen määrittäminen määräytyy pitkälti toimeksiantajaorganisaation nykyisen rakenteen ja asiakaskunnan mukaan. Lisäksi se määräytyy pysyvässä tai väliaikaisessa työsuhteessa olevien asiantuntijoiden saatavuuden mukaan.

CSIRT:ssä on tavallisesti määritetty seuraavat ryhmän sisäiset tehtävät:

Yleiset tehtävät

- toimitusjohtaja

Henkilöstö

- toimistopäällikkö
- kirjanpitäjä
- viestintäkonsultti
- oikeudellinen neuvonantaja

Toiminnallinen ja tekninen ryhmä

- Teknisen ryhmän johtaja
- CSIRT-palveluja tuottavat tekniset asiantuntijat
- tutkijat

Ulkoiset konsultit

- käytetään tarvittaessa

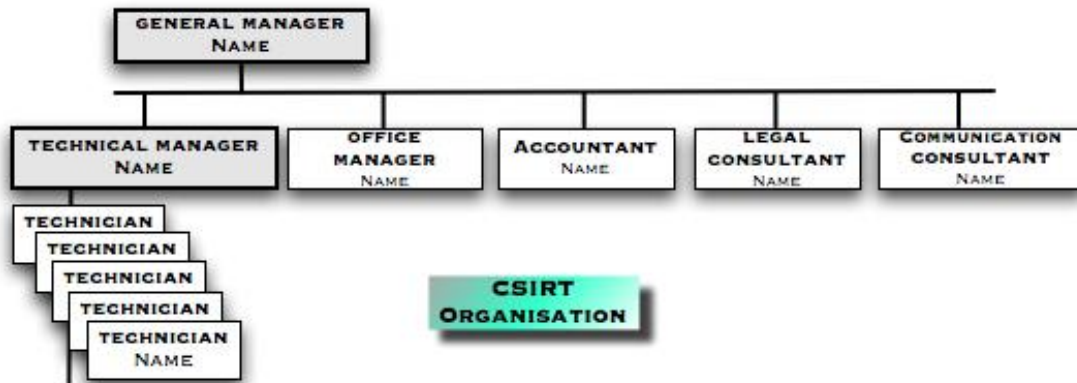
Etenkin CSIRT-ryhmän käynnistysvaiheessa oikeusalan asiantuntijan osallistuminen ryhmän toimintaan on erityisen tärkeää. Se lisää kustannuksia, mutta viime kädessä se säästää aikaa ja näin välttää oikeudellisilta ongelmilta.

Asiakaskunnan asiantuntemuksesta riippuen ja jos CSIRT-ryhmällä on suuri medianäkyvyys, viestintäasiantuntijan osallistuminen ryhmän toimintaan on osoittautunut hyvin järkeväksi. Viestintäasiantuntijat voivat esittää vaikeat tekniset kysymykset asiakaskunnan tai mediakumppaneiden kannalta ymmärrettävässä muodossa. Viestintäasiantuntijat välittävät myös asiakaskunnan antaman palautteen teknisille asiantuntijoille, joten he voivat toimia ”tulkkeina” tai ”välittäjinä” näiden kahden ryhmän välillä.

Seuraavassa esitetään muutamia esimerkkejä toiminnassa olevien CSIRT-ryhmien käyttämisestä organisaatiomalleista.

6..1 Itsenäisen organisaation malli

Perustettava CSIRT-ryhmä toimii itsenäisenä organisaationa, jolla on oma johtoelin ja henkilöstö.

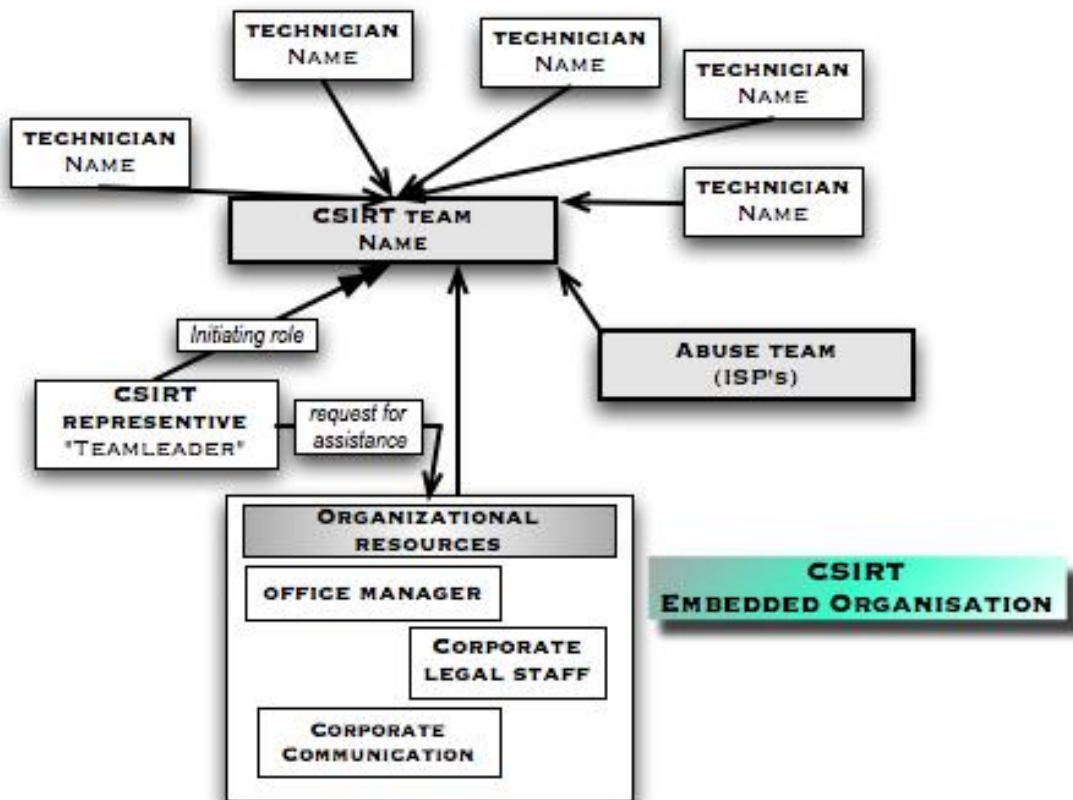


Kuva 5: Itsenäinen organisaatio

6..2 Integroidun organisaation malli

Tätä mallia voidaan soveltaa, jos CSIRT perustetaan jo toiminnassa olevan organisaation alaisuuteen hyödyntämällä esimerkiksi toiminnassa olevaa IT-osastoa. CSIRT-ryhmää johtaa ryhmänjohtaja (team leader), joka on vastuussa CSIRT:n toimista. Tietoturvaloukkausten käsittelyssä ja CSIRT-toimien toteuttamisessa ryhmänjohtaja kokoaa yhteen tarvittavat tekniset asiantuntijat. Hän voi pyytää tukea jo toiminnassa olevalta organisaatiolta asiantuntija-apua varten.

Tätä mallia voidaan myös mukauttaa mahdollisten erityistilanteiden mukaan. Tällöin ryhmän käyttöön osoitetaan tietty määrä täysipäiväisiä työntekijöitä (Full Time Equivalent, FTE). Esimerkin neuvontapisteen (abuse desk) hoitaminen on epäilemättä yhden tai (useimmiten) useamman FTE:n tehtävä.

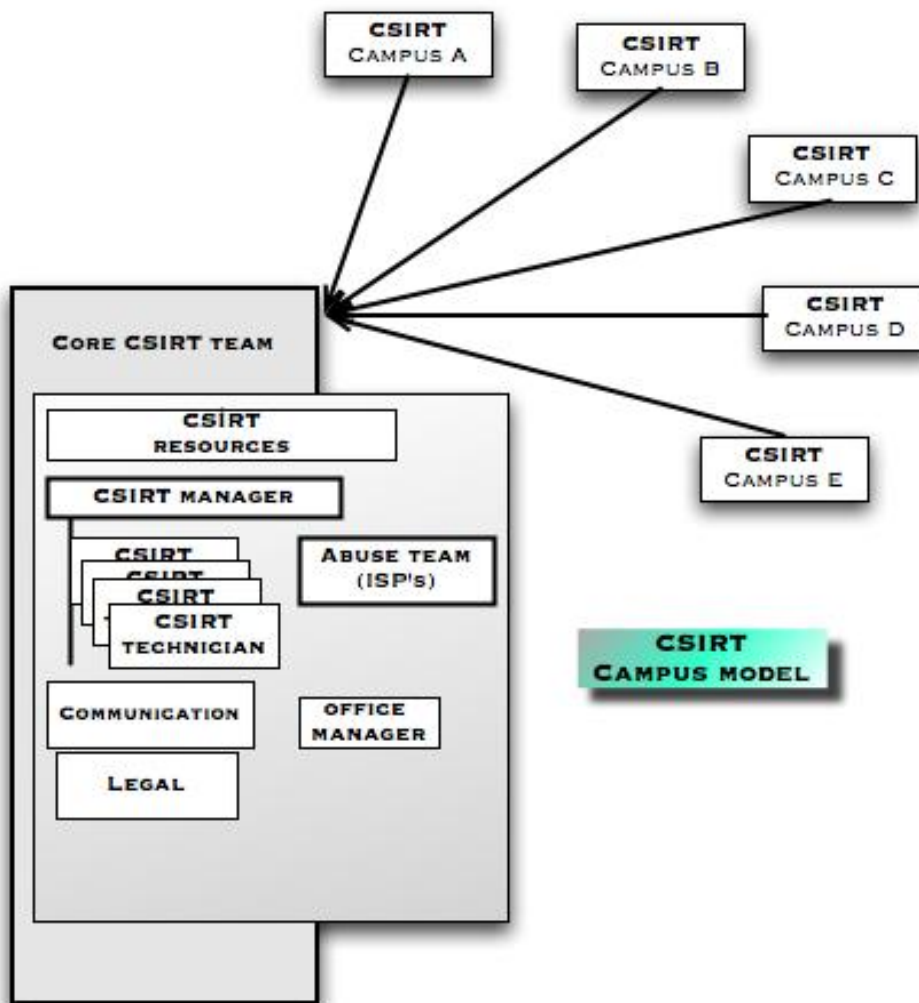


Kuva 6: Integroitu organisaatio

6..3 Kampusmalli

Kuten nimi viittaa, kampusmallia käyttävät useimmiten korkeakoulu- ja tutkimusalan CSIRT-ryhmät. Useimmat korkeakoulu- ja tutkimusorganisaatiot koostuvat useista korkeakouluista ja kampustiloista, jotka ovat levinneet eri puolille aluetta tai koko maan alueelle (kuten National Research Networks, NREN). Tavallisesti tällaiset organisaatiot ovat toisistaan riippumattomia, ja niillä on usein oma CSIRT-ryhmä. Tällaiset CSIRT-ryhmät on yleensä organisoitu yhden katto-organisaationa toimivan CSIRT:n alaisuuteen. Tämä katto-organisaationa toimiva CSIRT koordinoi toimia ja toimii yhteyspisteenä ulkomaailmalle. Tavallisesti katto-organisaationa toimiva CSIRT tarjoaa myös keskeisiä CSIRT-palveluja ja jakaa tietoturvaloukkauksia koskevaa tietoa kampusmalliin kuuluville CSIRT-ryhmille.

Jotkin CSIRT-ryhmät jakavat keskeiset CSIRT-palvelunsa muiden kampusmalliin kuuluvien CSIRT-ryhmien kanssa, minkä ansiosta katto-organisaationa toimivan CSIRT:n kokonaiskustannukset ovat pienemmät.



Kuva 7: Kampusmalli

6..4 Vapaaehtoisuuteen perustuva malli

Tässä organisaatiomallissa ryhmä henkilöitä (asiantuntijoita) kokoontuu yhteen antaakseen toisilleen (ja muille) neuvoja ja tukea vapaaehtoiselta pohjalta. Se on löyhästi organisoitunut yhteisö, joka on suuresti riippuvainen osallistujien motivaatiosta.

Esimerkiksi WARP-yhteisö¹³ (lyhenne englanninkielisistä sanoista **W**arning, **A**dvice **R**eporting **P**oints) perustuu tähän malliin.

Oikean henkilöstön palkkaaminen

Kun on päätetty, mitä palveluja ja minkä tasoista tukea tarjotaan ja mitä organisaatiomallia sovelletaan, seuraavassa vaiheessa on löydettävä oikea määrä pätevää henkilöstöä.

On lähes mahdotonta antaa tarkkoja tietoja kulloinkin tarvittavan teknisen henkilöstön määrästä, mutta seuraavat keskeiset arvot ovat osoittautuneet hyväksi ohjenuoraksi:

- Kahden keskeisen palvelun tarjoaminen, toisin sanoen tietoturvatiedotteiden laatiminen ja tietoturvaloukkausten käsittely: vähintään **4** täysipäiväistä työntekijää (FTE).
- CSIRT, joka tarjoaa kattavaa palvelua toimistoaikoina ja joka ylläpitää järjestelmiä: vähintään **6–8** täysipäiväistä työntekijää.
- Täysmiehitetty CSIRT, joka tarjoaa palveluja vuorokauden ympäri (24x7) (2 työvuorua toimistoaikojen ulkopuolella): vähintään noin **12** täysipäiväistä työntekijää.

Näissä luvuissa on otettu huomioon myös sairaustapausten, lomien ja muiden vastaavien takia palkattavat sijaiset. Tällöin on myös otettava huomioon alueelliset työehtosopimukset. Jos henkilöstö työskentelee toimistoaajan ulkopuolella, se voi aiheuttaa lisäkustannuksia maksettavien palkkalisien takia.

Jäljempänä esitetään pääpiirteittäin CSIRT-ryhmän teknisten asiantuntijoiden olennaiset pätevydet.

Teknisen henkilöstön yleinen työnkuvaus:

Henkilökohtaiset ominaisuudet

- joustavuus, luovuus ja hyvä ryhmähenki
- hyvä analysointikyky
- kyky esittää vaikeat tekniset asiat ymmärrettävästi

¹³ WARP-aloite http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

- kyky ymmärtää tietojen luottamuksellisuutta ja työskennellä jäsennellysti
- hyvä organisointikyky
- hyvä stressinsietokyky
- erinomaiset suulliset ja kirjalliset viestintätaidot
- avoin ja halukas oppimaan

Tekniset taidot

- Laaja tietämys Internet-teknologiasta ja -yhteyskäytännöistä
- Linux- ja Unix-järjestelmien tuntemus (asiakaskunnan laitteistojen mukaan)
- Windows-järjestelmien tuntemus (asiakaskunnan laitteistojen mukaan)
- Verkkoinfrastruktuuriin kuuluvien laitteiden tuntemus (reititin, kytkimet, DNS, välipalvelin, sähköposti jne.)
- Internet-sovellusten tuntemus (SMTP, HTTP(s), FTP, telnet, SSH jne.)
- tietoturvaohjelmien tuntemus (DDoS, verkkourkinta (phishing), sivujen töhriminen defacement-hyökkäyksillä, nuuskijaohjelmat (sniffing) jne.)
- Riskiarviointia koskeva tietämys ja käytännön toteutus

Lisätaidot ja -ominaisuudet

- Valmius työskennellä vuorokauden ympäri (24x7) tai päivystää (palvelumallin mukaan)
- Matkustushalukkuus (häätäpauksissa oltava käytettävissä toimistolla: pitkät matkaetäisyydet ja pitkät matkustusajat)
- Koulutustaso
- Työkokemusta IT-alan tietoturvasta

Kuvitteellinen CSIRT (vaihe 4)

Liiketoimintamallin määrittäminen

Rahoitusmalli

Koska yritys harjoittaa ympärivuorokautista (24x7) sähköistä liiketoimintaa ja sillä on ympäri vuorokauden toimiva IT-osasto, päätetään, että toimistoaikoina tarjotaan kattavaa palvelua ja toimistoaikojen ulkopuolella palveluja tarjotaan päivystysperiaatteella. Asiakaskunnalle tarjotaan palveluja maksutta, mutta mahdollisuutta tarjota palveluja myös ulkopuolisille asiakkaille tarkastellaan pilotti- ja arviointivaiheen aikana.

Tulomalli

Käynnistys- ja pilottivaiheen aikana CSIRT saa rahoitusta toimeksiantajayritykseltä. Pilotti- ja arviointivaiheen aikana keskustellaan lisärahoituksesta, johon liittyy myös mahdollisuus myydä palveluja ulkoisille asiakkaille.

Organisaatiomalli

Koska toimeksiantajaorganisaatio on pieni yritys, valitaan integroitu malli. Toimistoaikoina kolme työntekijää tarjoaa keskeisiä palveluja (tietoturvatiedotteiden laadinta ja tietoturvaloukkausten käsittely/koordinointi).

Yrityksen IT-osaston palveluksessa on jo asianmukaisesti pätevöitynyttä henkilöstöä. Osaston kanssa sovitaan, että uusi CSIRT-ryhmä voi pyytää tarvittaessa väliaikaista tukea. Lisäksi voidaan turvautua toissijaisesti päivystäviin teknisiin asiantuntijoihin.

CSIRT-ydinryhmä muodostuu neljästä täysipäiväisesti työskentelevästä jäsenestä ja viidestä CSIRT-ryhmän lisäjäsenestä. Yksi näistä jäsenistä on myös käytettävissä vuorotyötä varten.

Henkilöstö

CSIRT-ryhmän johtajalla on kokemusta tietoturvasta sekä ensimmäisen ja toisen tason tuesta ja kriisitilanteiden hallinnasta. Ryhmän muut kolme jäsentä ovat tietoturva-asiantuntijoita. IT-osastolla työskentelevät CSIRT-ryhmän osa-aikaiset jäsenet ovat asiantuntijoita omalla yrityksen infrastruktuurin vastuualueellaan.

Toimiston käyttö ja laitteisto

Toimiston laitteisto, käyttö ja fyysinen turvallisuus ovat hyvin monimutkaisia aiheita, eikä niitä voida tarkastella tyhjentävästi tässä asiakirjassa. Tässä luvussa on tarkoitus esittää suppea katsaus tähän aiheeseen.

Lisätietoa fyysisestä turvallisuudesta on saatavana seuraavilta verkkosivuilta:

http://en.wikipedia.org/wiki/Physical_security

http://www.sans.org/reading_room/whitepapers/physcial/

<http://www.infosyssec.net/infosyssec/physfac1.htm>

”Rakennuksen suojaaminen”

Koska CSIRT-ryhmät käsittelevät yleensä hyvin arkaluonteista tietoa, on suositeltavaa antaa ryhmälle vastuu toimiston fyysisestä turvallisuudesta. Toimiston suojaaminen riippuu pitkälti käytössä olevista välineistä ja infrastruktuurista ja toimeksiantajayrityksen tietoturvapoliitikasta.

Esimerkiksi valtiot käyttävät salassapitojärjestelmiä ja hyvin tiukkoja sääntöjä luottamuksellisen tiedon käsittelyssä. Alueella sovellettavat säännöt ja suuntaviivat on syytä tarkistaa omalta yritykseltä tai laitokselta.

Yleensä uuden CSIRT-ryhmän on turvauduttava yhteistyöhön toimeksiantajaorganisaationsa kanssa saadakseen tarkempaa tietoa paikallisista säännöistä, toimintalinjoista ja muista oikeudellisista kysymyksistä.

Tässä asiakirjassa ei esitetä tyhjentävää kuvausta kaikista tarvittavista laitteista ja turvatoimenpiteistä. Seuraavassa on kuitenkin lyhyt luettelo CSIRT-ryhmän peruslaitteistoista.

Rakennusta koskevat yleiset säännöt

- Valvotaan sisäänpääsyä.
- Varmistetaan, että CSIRT-toimistoon on pääsy ainoastaan CSIRT:n henkilökunnalla.
- Järjestetään kameravalvonta toimistoihin ja sisäänkäyntien yhteyteen.
- Arkistoidaan luottamukselliset tiedot lukittaviin kaappeihin tai tallelokeroon.
- Käytetään turvallisia IT-järjestelmiä.

IT-laitteistoja koskevat yleiset säännöt

- Käytetään laitteistoja, joiden käytössä henkilöstö voi antaa tukea.
- Suojataan kaikki järjestelmät.

- Korjataan (patch) ja päivitetään kaikki järjestelmät ennen niiden kytkemistä Internetiin.
- Käytetään tietoturvaohjelmistoja (palomureja, eri virustorjuntaohjelmia, vakoiluohjelmilta suojaavia ohjelmia jne.).

Viestintäkanavien ylläpito

- Julkinen verkkosivusto
- Vain jäsenille tarkoitettu Internet-sivusto
- Internet-lomakkeet tietoturvaloukkauksista raportoimiseksi
- Sähköposti (tuetaan PGP-, GPG-, S/MIME-menetelmiä)
- Postituslistaohjelmisto
- Asiakaskuntaa varten on käytössä oma puhelinnumero:
 - puhelin
 - faksi
 - tekstiviestit

Tiedonsaantijärjestelmät

- Yhteystietokanta, joka sisältää yksityiskohtaiset tiedot ryhmän jäsenistä, muista ryhmistä jne.
- Asiakkuudenhallintatyökalut (CRM tools)
- Ns. tikettijärjestelmä (ticket system) tietoturvaloukkausten käsittelyä varten

”Yritykselle ominaisen tyylin” soveltaminen alusta alkaen

- Sähköpostiviestien ja -tiedotteiden asetteluissa
- Paperikirjeissä
- Kuukausi- tai vuosiraporteissa
- Tietoturvaloukkausten raportointilomakkeissa

Muuta

- Kaistan ulkopuolinen viestintä hyökkäysten varalta
- Ylimääräiset Internet-yhteydet

Lisätietoa erityisistä CSIRT-työkaluista on luvussa 8.5 *”Käytettävissä olevat CSIRT-työkalut”*.

Tietoturvapolitiikan laatiminen

CSIRT-ryhmän organisaatiomallin mukaan sovelletaan räätälöityä tietoturvapolitiikkaa. Sen lisäksi, että tällaisessa toimintapolitiikassa kuvataan toivotut toiminnan ja hallinnon menetelmät ja menettelyt, sen on noudatettava lainsäädäntöä ja standardeja, etenkin CSIRT-ryhmän vastuuvollisuuden osalta. CSIRT-ryhmää sitovat tavallisesti kansalliset lait ja määräykset, jotka pannaan usein täytäntöön Euroopan unionin lainsäädännön (yleensä direktiivien) ja muiden kansainvälisten sopimusten rajoissa. Standardit eivät ole välttämättä sitovia, mutta ne voidaan kuitenkin määrätä tai suositella täytäntöönpantavaksi lakien ja määräysten avulla.

Jäljempänä esitetään lyhyt luettelo mahdollisista laeista ja toimintalinjoista:

Kansallisella tasolla

- Tietotekniikkaa, televiestintää ja tiedotusvälineitä koskevat eri lait
- Tietosuojaa ja yksityisyyttä koskevat lait
- Tietojen säilyttämistä koskevat lait ja määräykset
- Rahoitusta, kirjanpitoa ja yrityshallintoa koskeva lainsäädäntö
- Yrityshallintoa ja IT-hallintoa koskevat käytäntönsäännöt

Euroopan unionin tasolla

- Sähköisistä allekirjoituksista annettu direktiivi (1999/93/EY)
- Tietosuojadirektiivi (1995/46/EY) ja sähköisen viestinnän tietosuojadirektiivi (2002/58/EY)
- Sähköisistä viestintäverkoista ja -palveluista annetut direktiivit (2002/19/EY – 2002/22/EY)
- Yhtiöoikeutta koskevat direktiivit (esim. kahdeksas yhtiöoikeusdirektiivi)

Kansainvälisellä tasolla

- Basel II -sopimus (etenkin toiminnallisten riskien hallinnoinnin osalta)
- Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus
- Euroopan neuvoston ihmisoikeusyleissopimus (tietosuojaa koskeva 8 artikla)
- Kansainväliset tilinpäätösstandardit (International Accounting Standards, IAS, joissa määrätään tietyistä IT-tarkastuksista)

Standardit

- Brittiläinen standardi BS 7799 (tietoturva)
- Kansainväliset standardit ISO2700x (tietoturvahallintajärjestelmät)
- Saksan IT-Grundschutzbuch, Ranskan EBIOS ja muut kansalliset versiot

Sen varmistamiseksi, toimiiko oma CSIRT-ryhmä kansallisen ja kansainvälisen lainsäädännön mukaisesti, on syytä kääntyä oikeudellisen neuvonantajan puoleen.

Tiedonkäsittelypolitiikassa on vastattava seuraaviin peruskysymyksiin:

- Miten tuleva tieto ”merkitään” (tags) tai ”luokitellaan”?

- Miten tietoa käsitellään, etenkin luottamuksellisuuden näkökulmasta?
- Mitkä näkökohdat otetaan huomioon tietoja paljastettaessa etenkin, jos tietoturvaloukkauksiin liittyvää tietoa välitetään muille ryhmille tai muihin sijainteihin?
- Onko tietojen käsittelyssä otettava huomioon oikeudellisia näkökulmia?
- Onko laadittu suuntaviivoja salauksen käytöstä arkistojen ja/tai tietoliikenteen (etenkin sähköpostin) luottamuksellisuuden ja eheyden suojelemiseksi?
- Sisältyykö näihin suuntaviivoihin mahdollisia oikeudellisia reunaehdoja, kuten vara-avainjärjestelmä tai salauksen purkamisen toteutus oikeuskannetapauksissa.

Kuvitteellinen CSIRT (vaihe 5)

Toimiston laitteistot ja sijainti

Koska toimeksiantajayrityksellä on jo käytössä tehokas fyysinen turvajärjestelmä, uusi CSIRT-ryhmä on tältä osin hyvin turvattu. Hätätilanteissa tehtävää koordinoitua varten otetaan käyttöön niin kutsuttu "war room" -neuvottelutila. Salausaineistoa ja arkaluonteisia asiakirjoja varten hankitaan tallelokero. Lisäksi otetaan käyttöön erillinen puhelinlinja ja vaihde, jotta helpotetaan hotline-palvelun toimintaa toimistoaikoina, ja "päivystävä" matkapuhelin, johon vastataan toimistoajan ulkopuolella ja jonka puhelinnumero on sama.

Jo käytössä olevia laitteita ja yrityksen verkkosivuja voidaan hyödyntää CSIRT:hen liittyvistä kysymyksistä tiedottamiseksi. Lisäksi otetaan käyttöön ja pidetään yllä postituslistaa, ja ryhmän jäsenten välistä sekä muiden ryhmien kanssa harjoitettavaa viestintää varten perustetaan rajoitettu foorumi. Kaikkien henkilöstön jäsenten yhteystiedot tallennetaan tietokantaan, ja tulostettuja tietoja säilytetään tallelokerossa.

Sääntely

Koska CSIRT-ryhmä integroidaan osaksi yritystä, jolla on jo käytössä oma tietoturvapoliittikka, CSIRT-ryhmää koskeva vastaava politiikka määritetään yrityksen oikeudellisen neuvonantajan kanssa.

Yhteistyömahdollisuudet muiden CSIRT-ryhmien ja mahdollisten kansallisten aloitteiden kanssa

Tässä asiakirjassa on jo viitattu muutaman kerran muihin CSIRT-aloitteisiin ja suureen tarpeeseen tehdä niiden kanssa yhteistyötä. On osoittautunut hyväksi käytännöksi ottaa mahdollisimman varhaisessa vaiheessa yhteyttä muihin CSIRT-ryhmiin tarpeellisten yhteyksien luomiseksi CSIRT-yhteisöihin. Yleensä muut CSIRT-ryhmät ovat hyvin halukkaita auttamaan vastaperustettuja ryhmiä pääsemään alkuun.

ENISAn laatima CERT-toimien luettelo "*Inventory of CERT activities in Europe*"¹⁴ on hyvä lähtökohta saman maan muiden CSIRT-ryhmien tai kansallisten CSIRT-ryhmien yhteistyömahdollisuuksien kartoittamiselle.

Sopivien CSIRT-tietolähteiden löytämiseksi saa apua ENISAn CSIRT-asiantuntijoilta:

CERT-Relations@enisa.europa.eu

¹⁴ ENISAn luettelo: http://www.enisa.europa.eu/cert_inventory/

Jäljempänä on yhteenveto CSIRT-yhteisötoimista. Kattava kuvaus ja lisätietoa löytyy edellä mainitusta ENISAn luettelosta.

Eurooppalainen CSIRT-aloite

TF-CSIRT¹⁵

TF-CSIRT-työryhmän tehtävänä on edistää CSIRT-tietoturvaryhmien välistä yhteistyötä Euroopassa. Tämän työryhmän keskeisinä tavoitteina on tarjota foorumi kokemusten ja tietojen vaihtamiseksi, tarjota pilottipalveluja Euroopan CSIRT-yhteisölle ja avustaa uusien CSIRT-ryhmien perustamisessa.

Työryhmän tärkeimmät tavoitteet ovat seuraavat:

- Tarjota foorumi kokemusten ja tietojen vaihtamiseksi
- Tarjota pilottipalveluja Euroopan CSIRT-yhteisölle
- Edistää yhteisiä standardeja ja menettelyjä tietoturvaloukkausten käsittelemiseksi
- Avustaa uusien CSIRT-ryhmien perustamisessa ja CSIRT-henkilöstön kouluttamisessa.
- TF-CSIRT:n toimien painopiste on Euroopassa ja naapurimaissa TERENAn (Trans-European Research and Education Association) 15. syyskuuta 2004 hyväksymien toimintaehtojen mukaiseksi.

Maailmanlaajuinen CSIRT-aloite

FIRST¹⁶

FIRST (Forum of Incident Response and Security Teams) on maailmanlaajuisesti tunnettu johtava järjestö tietoturvan alalla. FIRST:n jäsenenä tietoturvaryhmät voivat reagoida tehokkaammin tietoturvaloukkauksiin – niin reaktiivisesti kuin proaktiivisestikin.

FIRSTiin kuuluu monenlaisia valtionhallinnon, kaupallisten organisaatioiden ja koulutusorganisaatioiden tietoturvaryhmiä. FIRST-järjestön tavoitteena on edistää yhteistyötä ja koordinoitua tietoturvaloukkausten estämiseksi, nopeuttaa tietoturvaloukkausten käsittelyä ja edistää tiedon jakamista jäsenten ja koko yhteisön kesken.

Sen lisäksi, että FIRST-järjestö muodostaa kansainvälisen tietoturvayhteisön toimintaverkoston, se tarjoaa myös lisäarvoa tuottavia palveluja.

Kuvitteellinen CSIRT (vaihe 6)

Yhteistyömahdollisuuksien etsintä

ENISAn luettelon avulla löytyi nopeasti samassa maassa toimivia CSIRT-ryhmiä, joihin otettiin yhteyttä. Sovittiin, että uusi ryhmänjohtaja vierailee yhdessä näistä ryhmistä. Tämän vierailun yhteydessä hän sai tietoa kansallisista CSIRT-toimista ja osallistui kokokseen.

Kokous osoittautui erittäin hyödylliseksi, sillä näin ryhmänjohtaja sai tietoa työskentelymenetelmistä ja tukea muutamalta muulta ryhmältä.

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 Liiketoimintasuunnitelman edistäminen

Tähän mennessä on toteutettu seuraavat vaiheet:

1. Mikä on CSIRT ja mitä hyötyä siitä on?
2. Mille toimialalle uusi ryhmä tarjoaa palveluja?
3. Mitä palveluja CSIRT-ryhmä voi tarjota asiakaskunnalleen
4. Toimintaympäristön ja asiakkaiden arviointi
5. Toimenkuvan määrittäminen
6. Liiketoimintasuunnitelman laatiminen
 - a. Rahoitusmallin määrittäminen
 - b. Organisaatorakenteen määrittäminen
 - c. Henkilökunnan rekrytoinnin aloittaminen
 - d. Toimiston käyttö ja laitteisto
 - e. Tietoturvalähtöisen toiminnan laatiminen
 - f. Yhteistyökumppaneiden etsiminen

>> Seuraavaksi edellä esitetyt vaiheet sisällytetään hankesuunnitelmaan ja ryhdytään toimeen.

On suositeltavaa aloittaa hankkeen määrittely laatimalla liiketoimintasuunnitelma. Tätä liiketoimintasuunnitelmaa käytetään hankesuunnitelman perustana tai silloin, kun pyydetään johdon tukea tai rahoitusta tai muita resursseja.

Jatkuva raportointi johdolle on osoittautunut hyväksi keinoksi ylläpitää tietoisuutta tietoturvaongelmista ja saada samalla jatkuvasti tukea CSIRT-ryhmälle.

Liiketoimintasuunnitelma käynnistetään analysoimalla ongelmat ja mahdollisuudet luvussa 5.3 ”*Asiakaskunnan analysointi*” kuvatun analyysimallin avulla ja luomalla tiivis yhteys mahdolliseen asiakaskuntaan.

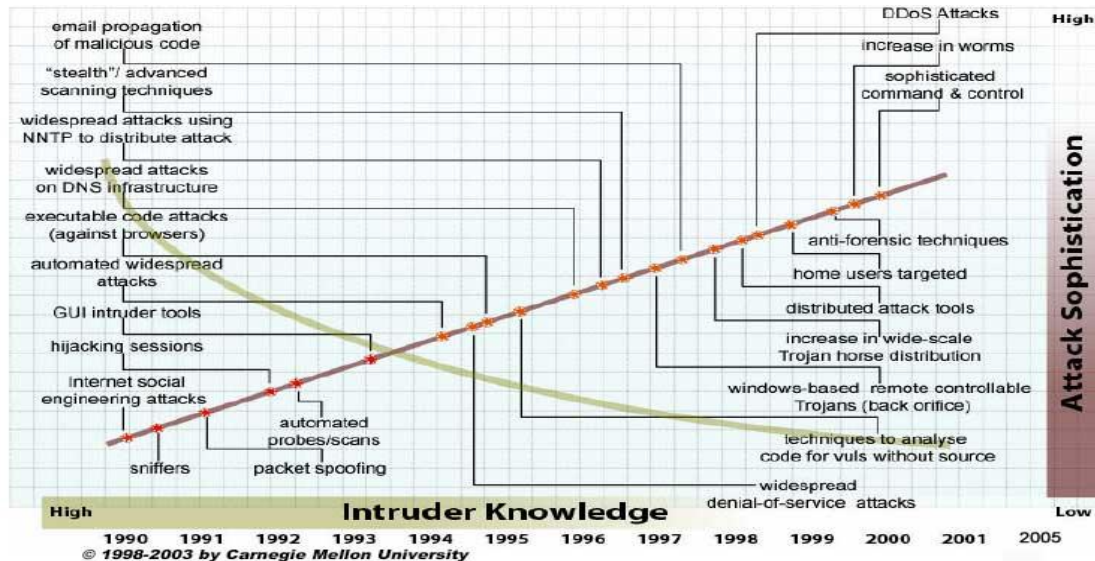
Kuten aiemmin on todettu, CSIRT-ryhmän perustamisessa on otettava huomioon monia eri tekijöitä. Parasta on mukauttaa edellä mainittu aineisto CSIRT-ryhmän tarpeisiin sitä mukaa kuin tarpeita ilmenee.

Yrityksen johdolle raportoitessa on suositeltavaa laatia mahdollisimman ajantasainen suunnitelma käyttämällä hiljattain ilmestyneitä sanomalehtiartikkeleita tai Internetiä ja selittää, miksi CSIRT-ryhmän palvelut ja tietoturvaloukkausten sisäinen koordinointi ovat erittäin tärkeitä liiketoiminnan varojen turvaamisen kannalta. On myös tarpeen selvittää, että vakaa liiketoiminta edellyttää tietotekniikka-alan turvallisuuskysymysten jatkuvaa tarkastelua varsinkin, jos kyse on tietotekniikasta riippuvaisista yrityksistä tai laitoksista.

(Bruce Schneierin kuuluisa toteamus kiteyttää tämän ajatuksen: ”*Tietoturva ei ole tuote vaan prosessi*”¹⁷)

¹⁷ Bruce Schneier: <http://www.schneier.com/>

Seuraava CERT/CC:n laatima kaavio on tunnettu työkalu, jolla kuvataan tietoturvaongelmia:



Kuva 8: Tunkeutujan tietojen vertaaminen hyökkäyksen monimutkaisuuteen (lähde CERT-CC¹⁸)

Kaaviossa kuvataan IT-alan tietoturvaan liittyviä suuntauksia. Eräs tällainen suuntaus on se, että yhä kehittyneempien hyökkäysten toteuttamiseen tarvitaan yhä vähemmän taitoja.

Eräs toinen mainitsemisen arvoinen seikka on se, että heikkojen kohtien korjaamiseksi suoritettavien ohjelmistopäivitysten ja ohjelmistoihin kohdistuvien hyökkäysten alkamisen välinen aika on yhä lyhyempi.

Korjaus (patch) -> Väärinkäyttö

Nimda:	11 kuukautta
Slammer:	6 kuukautta
Nachi:	5 kuukautta
Blaster:	3 viikkoa
Witty:	1 päivä (!)

Leviämisnopeus

Code red:	päiviä
Nimda:	tunteja
Slammer:	minuutteja

Kootuista tietoturvaloukkauksia koskevista tiedoista, mahdollisista parannuksista ja saaduista kokemuksista voidaan myös laatia hyvä kuvaus.

Liiketoimintasuunnitelmien kuvaus ja johdon kannustaminen toimimaan

Pelkästään johdolle suunnattu raportti, CSIRT-ryhmän mainostaminen mukaan luettuna, ei vielä käy liiketoimintasuunnitelmasta, mutta jos se laaditaan oikein, johtoelin antaa useimmiten lopulta tukensa CSIRT-ryhmälle. Liiketoimintasuunnitelmaa ei toisaalta tulisi

¹⁸ <http://www.cert.org/archive/pdf/info-sec-ip.pdf>

pitää ainoastaan johdolle suunnattuna, vaan sitä tulisi käyttää myös ryhmän ja asiakaskunnan kanssa käytävän viestinnän lähtökohtana. Termi liiketoimintasuunnitelma voi kuulostaa hyvin kaupalliselta ja etäiseltä CSIRT-ryhmän päivittäisen toiminnan näkökulmasta, mutta se on hyvä lähtökohta CSIRT-ryhmän perustamista varten.

Vastauksia seuraaviin kysymyksiin voidaan käyttää hyvän liiketoimintasuunnitelman suunnittelussa (annetut esimerkit ovat kuvitteellisia, ja niitä käytetään vain havainnollistamiseksi; ”oikeat” vastaukset riippuvat täysin ”todellisista” olosuhteista).

- Mikä on ongelmana?
- Mitkä tavoitteet halutaan saavuttaa asiakaskunnan kanssa?
- Mitä tapahtuu, jos ei tehdä mitään?
- Mitä tapahtuu, jos ryhdytään toimiin?
- Mitä tämä maksaa?
- Mitä tällä saavutetaan?
- Milloin aloitetaan ja milloin lopetetaan?

Mikä on ongelmana?

Useimmissa tapauksissa ajatus CSIRT-ryhmän perustamisesta syntyy, kun tietoturvasta on tullut olennainen osa yrityksen tai laitoksen pääasiallista toimintaa ja kun tietoturvaloukkauksista muodostuu liiketoimintariski, minkä vuoksi turvatoimenpiteistä tulee osa tavanomaista liiketoimintaa.

Valtaosalla yrityksistä tai laitoksista on asianmukainen tukiosasto tai käyttötuki, mutta useimmiten tietoturvaloukkauksia ei käsitellä riittävästi eikä riittävän järjestelmällisesti. Useimmissa tapauksissa tietoturvaloukkausten käsittely edellyttää erityisiä taitoja ja erityistä huomiota. Järjestelmällisestä lähestymistavasta koituu hyötyä, ja se vähentää yritykselle aiheutuvia liiketoimintariskejä ja vahinkoja.

Ongelmana on useimmissa tapauksissa koordinoinnin puute ja se, ettei saatavana olevaa tietoa käytetä tietoturvaloukkausten käsittelyssä, mikä voisi estää tulevat tietoturvaloukkaukset ja mahdolliset taloudelliset tappiot ja/tai laitoksen maineen vahingoittumisen.

Mitkä tavoitteet halutaan saavuttaa asiakaskunnan kanssa?

Kuten aikaisemmin on todettu, CSIRT-ryhmä palvelee asiakaskuntaansa ja auttaa sitä ratkaisemaan tietoturvaloukkaukset ja -ongelmat. IT-alan tietoturvakysymyksiä koskevan tietämyksen parantaminen ja tietoturvatietoisuutta edistävän kulttuurin aikaansaaminen ovat lisätavoitteita.

Tällaisessa kulttuurissa pyritään toteuttamaan ennakoivia ja ehkäiseviä toimenpiteitä heti alkuvaiheessa ja vähentämään siten toimintakustannuksia.

Tällaisen yhteistyö- ja avunantokulttuurin käyttöönotto yrityksessä tai laitoksessa voi useimmissa tapauksissa edistää tehokkuutta yleisesti.

Mitä tapahtuu, jos ei tehdä mitään?

Jos tietoturvaan ei omaksuta järjestelmällistä käsittelytapaa, se voi aiheuttaa lisävahinkoja, eikä vähiten laitoksen maineelle. Tämä voi johtaa myös taloudellisiin tappioihin ja oikeudellisiin seurauksiin.

Mitä tapahtuu, jos ryhdytään toimiin?

Tietoisuus tietoturvaongelmista kasvaa. Tämä helpottaa ongelmien ratkaisemista tehokkaammin ja estää tulevia menetyksiä.

Mitä tämä maksaa?

Organisaatiomallin mukaan kustannuksia aiheutuu CSIRT-ryhmän jäsenten ja CSIRT-organisaation henkilöstökuluista sekä laitteista, työkaluista ja ohjelmistolisensseistä.

Mitä hyötyä tästä on?

Liiketoiminta-alasta ja aiemmista menetyksistä riippuen menettelyt ja turvakäytännöt muuttuvat avoimemmiksi, ja siten suojellaan yrityksen tärkeää omaisuutta.

Mitkä ovat aikarajat?

Hankesuunnitelmaa koskeva malli on kuvattu luvussa 12 "*Hankesuunnitelman kuvaus*".

Esimerkkejä nykyisistä liiketoimintasuunnitelmista ja lähestymistavoista

Seuraavassa on CSIRT-ryhmän liiketoimintasuunnitelmista joitakin esimerkkejä, joita kannattaa tutkia:

- http://www.cert.org/csirts/AFI_case-study.html
Rahoituslaitoksen CSIRT-ryhmän perustaminen: tapaustutkimus

Tässä asiakirjassa esitetään erään rahoituslaitoksen (tässä asiakirjassa AFI) kokemuksia turvallisuusongelmia käsittelevän suunnitelman ja tietoturvaloukkauksia käsittelevän ryhmän (Computer Security Incident Response Team, CSIRT) kehittämisestä ja käyttöönotosta.
- <http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>
CERT POLSKAn yhteenveto liiketoimintasuunnitelmasta (diaesitys PDF-muodossa).
- <http://www.auscert.org.au/render.html?it=2252>
IRT-ryhmän (Incident Response Team) perustaminen saattoi olla vaikeaa 1990-luvulla. Monilla tietoturvaryhmän perustamiseen osallistuvilla henkilöillä ei ole siitä kokemusta. Tässä asiakirjassa tutkitaan IRT-ryhmän tehtävää yhteiskunnassa ja kysymyksiä, joita pitäisi käsitellä sekä toimia suunniteltaessa että toimien aloittamisen jälkeen. Tästä voi olla hyötyä toiminnassa oleville IRT-ryhmille, sillä näin voidaan lisätä tietämystä aiemmin käsittelemättömistä asioista.
- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
Tietoturvallisuuden tapaustutkimus, yrityksen turvaaminen: Roger Benton

Tämä tapaustutkimus koskee vakuutusyhtiötä, joka siirtyi koko yrityksen kattavaan tietoturvajärjestelmään. Siinä esitetään eri vaiheita, joita noudatetaan tietoturvajärjestelmää perustettaessa tai siihen siirryttäessä. Alussa alkeellinen online-tietoturvajärjestelmä oli ainut mekanismi, jolla valvottiin pääsyä yrityksen

tietoihin. Riskit olivat suuret – online-ympäristön ulkopuolella ei ollut valvottu tietojen eheyttä. Kuka tahansa, jolla oli ohjelmoinnin perustaidot, pystyi lisäämään, muuttamaan ja/tai poistamaan tuotantotietoja.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
Marriott-yrityksen sähköisen turvallisuuden strategia: yritysten ja tietotekniikka-alan välinen yhteistyö

Chris Zoladzin (Marriott International, Inc) kokemusten mukaan sähköisen kaupankäynnin turvallisuus ei ole yksittäinen hanke vaan prosessi. Tällaisen viestin Zoladz esitti Bostonissa äskettäin järjestetyssä sähköistä turvallisuutta käsittelevässä konferenssissa (E-Security Conference and Expo), jota sponsoroi Intermedia Group. Marriott-yrityksen tietoturvaluusyksikön varatoimitusjohtaja Zoladz hoitaa raportoinnin oikeudellisen osaston alaisuudessa, vaikkei hän olekaan juristi. Hänen tehtävänsä on määrittää, mihin Marriott-yrityksen arvokkaimmat liike-tiedot tallennetaan ja miten tietoja siirretään yrityksen sisällä ja ulkopuolella. Marriott-yrityksessä tietoturvaa tuetaan erikseen teknisellä infrastruktuurilla, ja tämä tehtävä on annettu tietoturva-arkkitehdille.

Kuvitteellinen CSIRT (vaihe 7)

Liiketoimintasuunnitelman edistäminen

Yrityksen historiasta on päätetty kerätä tietoja ja lukuja, mistä on valtavasti hyötyä IT-alan tietoturvatilannetta koskevaa tilastokatsausta laadittaessa. Tietojen ja lukujen keräämistä pitäisi jatkaa, kun CSIRT-ryhmä on perustettu ja toiminnassa, jotta tilastot pysyvät ajan tasalla.

Muihin kansallisiin CSIRT-ryhmiin otettiin yhteyttä, ja niitä haastateltiin liiketoimintasuunnitelmien osalta. Ne tarjosivat tukea kokoamalla diaesityksiä, joissa oli tietoa tietoturvaloukkausten viimeaikaisesta kehityksestä ja tietoturvaloukkausten kustannuksista.

Tässä kuvitteellisessa CSIRT-ryhmän esimerkkitapauksessa ei ollut pakottavaa tarvetta saada johtoa vakuuttuneeksi IT-toiminnan tärkeydestä, joten ei ollut vaikea saada suostumusta ensimmäiselle vaiheelle. Tämän jälkeen laadittiin liiketoiminta- ja hankesuunnitelma sekä arvio perustamis- ja toimintakustannuksista.

8 Esimerkkejä toiminnallisista ja teknisistä menettelyistä (työnkulku)

Tähän mennessä on toteutettu seuraavat vaiheet:

1. Mikä on CSIRT ja mitä hyötyä siitä on?
2. Mille toimialalle uusi ryhmä tarjoaa palveluja?
3. Mitä palveluja CSIRT-ryhmä voi tarjota asiakaskunnalleen?
4. Toimintaympäristön ja asiakkaiden arviointi
5. Toimenkuvan määrittäminen
6. Liiketoimintasuunnitelman laatiminen
 - a. Rahoitusmallin määrittäminen
 - b. Organisaatorakenteen määrittäminen
 - c. Henkilökunnan rekrytoinnin aloittaminen
 - d. Toimiston käyttö ja laitteistot
 - e. Tietoturvapoliitikan laatiminen
 - f. Yhteistyökumppaneiden etsiminen
7. Liiketoimintasuunnitelman edistäminen
 - a. Liiketoimintasuunnitelman hyväksyttäminen
 - b. Eri osien sisällyttäminen hankesuunnitelmaan

>> Seuraavassa vaiheessa CSIRT-ryhmä aloittaa toimintansa.

Hyvin laadituilla työkulkukaavioilla parannetaan laatua ja vähennetään tietoturvaloukkausten tai heikon kohdan käsittelyyn tarvittavaa aikaa.

Kuten esimerkikilaatikoissa on todettu, kuvitteellisen CSIRT-ryhmän tarjoamia keskeisiä CSIRT-peruspalveluja ovat:

- hälytykset ja varoitukset
- tietoturvaloukkausten käsittely
- tiedotteet.

Tässä luvussa esitetään esimerkkejä CSIRT-ryhmän keskeisiä palveluja kuvaavista työkuluista. Tämä luku sisältää myös tietoa tietojen keräämisestä eri lähteistä, tietojen merkityksellisyydestä ja aitoudesta sekä tiedon jakamisesta asiakaskunnalle. Tämän luvun lopussa on esimerkkejä perusmenettelyistä ja erityisistä CSIRT-työkaluista.

Asiakaskunnan IT-järjestelmän arvioiminen

Ensimmäiseksi on luotava yleiskatsaus asiakaskunnan käytössä oleviin IT-järjestelmiin. Näin CSIRT-ryhmä voi arvioida saamansa tiedon merkityksellisyyttä ja suodattaa sitä ennen tiedon levittämistä, jotta asiakkaita ei kuormiteta hyödyttömällä tiedolla.

Hyvä käytäntö on aloittaa yksinkertaisella menetelmällä ja käyttää esimerkiksi seuraavanlaista Excel-taulukkoa:

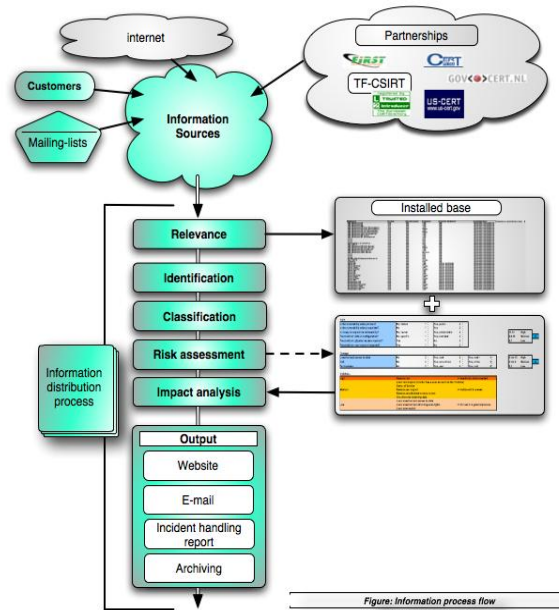
Luokka	Sovellus	Ohjelmisto-tuote	Versio	Käyttö-järjestelmä	Käyttö-järjestelmän versio	Kohde-ryhmä
Sovellus	Toimisto	Excel	x-x-x	Microsoft	XP-prof	A
Sovellus	Selain	IE	x-x-	Microsoft	XP-prof	A
Verkko	Reititin	CISCO	x-x-x	CISCO	x-x-x-	B
Palvelin	Palvelin	Linux	x-x-x	L-distro	x-x-x	B
Palvelut	WWW-palvelin	Apache		Unix	x-x-x	B

Excelin suodatustoiminnon avulla on erittäin helppo valita oikea ohjelmisto ja tunnistaa, mitä ohjelmistoa kukin asiakas käyttää.

Hälytysten, varoitusten ja tiedotteiden tuottaminen

Hälytysten, varoitusten ja tiedotteiden tuottamisessa noudatetaan samaa työkulkua:

- Tiedon kerääminen
- Tiedon merkityksellisyyden ja lähteiden arviointi
- Kerättyyn tietoon perustuva riskinarviointi
- Tiedon jakaminen



Kuva 9: Tietojen käsittelyn kulku

Tätä työkulkua kuvataan tarkemmin seuraavissa kohdissa.

1

Vaihe 1: Heikkoja kohtia koskevien tietojen kerääminen

Yleensä CSIRT-palvelujen tuottamisessa käytetään kahta päätietolähdettä:

- IT-järjestelmien heikkoja kohtia koskevat tiedot
- Tietoturvaloukkauksia koskevat raportit

Liiketoimintatyyppistä ja IT-järjestelmästä riippuen voidaan käyttää monia julkisia ja rajoitettuja lähteitä, joista saa heikkoja kohtia koskevaa tietoa:

- Julkiset ja rajoitetut postituslistat
- Palveluntarjoajien tiedot tuotteiden heikoista kohdista
- WWW-sivustot

- Internetissä olevat tiedot (Google jne.)
- Julkisen ja yksityisen sektorin yhteistyötahot, joilta saa tietoja heikoista kohdista (FIRST, TF-CSIRT, CERT-CC, US-CERT jne.)

Kaikki nämä tiedot lisäävät tietämystä IT-järjestelmien heikoista kohdista.

Kuten edellä on todettu, Internetissä on paljon hyviä ja helposti saatavia turvallisuustietolähteitä. Tätä asiakirjaa kirjoitettaessa ENISAn tilapäinen työryhmä "CERT Services" laati tietolähteistä kattavaa luetteloa, jonka oli määrä olla valmis vuoden 2006 lopussa.¹⁹

2

Vaihe 2: Tietojen ja riskien arviointi

Tässä vaiheessa arvioidaan, miten jokin tietty heikko kohta vaikuttaa asiakaskunnan IT-infrastruktuuriin.

Tunnistaminen

Saatujen heikkoja kohtia koskevien tietojen lähde on aina tunnistettava, ja on määriteltävä, onko lähde luotettava ennen kuin tiedot välitetään asiakaskunnalle. Muuten voidaan antaa vääriä hälytyksiä, mikä voi johtaa tarpeettomiin häiriöihin liiketoimintamenettelyissä ja lopulta vahingoittaa CSIRT-ryhmien mainetta.

¹⁹ Tilapäinen työryhmä CERT Services: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Seuraavassa menettelyssä esitetään yksi tapa tunnistaa viestin aitous:

Viestin aitouden ja sen lähteen tunnistaminen

Yleinen tarkistuslista

1. Onko lähde tunnettu ja rekisteröity?
2. Tuleeko tieto tavanomaisen kanavan kautta?
3. Sisältääkö viesti "outoa" tietoa, joka "tuntuu" väärältä?
4. Jos sinulla on epäilyksen tunne, että tiedot voivat olla vääriä, älä jatka, vaan varmista ne uudestaan.

Sähköpostiviestien lähteet

1. Tunteeko organisaatio lähdeosoitteen ja onko lähdeosoite lähdeluettelossa?
2. Onko PGP-allekirjoitus oikea?
3. Jos asia on epäselvä, tarkista viestin täydelliset otsikkotiedot.
4. Jos asia on epäselvä, käytä "nslookup"- tai "dig"-komentoa lähettäjän verkkotunnuksen vahvistamiseksi.²⁰

WWW-lähteet

1. Tarkista selaimen varmistukset, kun kytkeydyt suojattuun WWW-sivustoon (https://).
2. Tarkista lähteen sisältö ja käyttökelpoisuus (teknisestä näkökulmasta).
3. Jos asia on epäselvä, älä napsauta linkkejä tai lataa ohjelmistoja.
4. Jos asia on epäselvä, käytä "lookup"- ja "dig"-komentoa verkkotunnuksen tarkistamiseksi ja suorita "traceroute"-komento.

Puhelin

1. Kuuntele tarkkaan nimi.
2. Tunnistatko äänen?
3. Mikäli asia on epäselvä, kysy soittajan puhelinnumeroa voidaksesi soittaa hänelle takaisin.

Kuva 10: Esimerkki tietojen tunnistamisen menettelystä

Merkityksellisyys

Aiemmin laadittua asennettuja laitteistoja ja ohjelmistoja koskevaa yleiskatsausta voidaan käyttää heikkoja kohtia koskevien tietojen suodattamiseen merkityksellisyyden perusteella. Tavoitteena on löytää vastaus kysymyksiin: "Käyttääkö asiakaskunta tätä ohjelmistoa?" tai "Onko tieto merkityksellinen asiakkaille?"

Luottamuksellisuus

Saadut tiedot on ehkä luokiteltu tai merkitty luottamuksellisiksi (esimerkiksi tulevat tietoturvaloukkauksia koskevat raportit muilta ryhmiltä). Kaikki tiedot on käsiteltävä lähettäjän pyynnön ja oman tietoturvapoliittikan mukaisesti. Hyvä perussääntö on "Älä jaa tietoa, jos on epäselvää, voiko tietoa jakaa eteenpäin. Epäselvissä tapauksissa pyydä lähettäjältä lupa."

²⁰ Työkalut identiteettien tarkistamiseksi CHIHT:ssä: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Riskien ja vaikutusten arviointi

On useita menetelmiä (mahdollisen) heikon kohdan aiheuttaman riskin ja sen vaikutusten arvioimiseksi.

Riskillä tarkoitetaan mahdollisuutta hyödyntää heikkoa kohtaa. Arvioinnissa on otettava huomioon monia tärkeitä tekijöitä, muun muassa seuraavat:

- Onko heikko kohta yleisesti tiedossa?
- Onko järjestelmän heikkous levinnyt laajalle?
- Onko heikkoa kohtaa helppo käyttää hyväksi?
- Voiko kyseistä heikkoa kohtaa käyttää hyväksi etäältä?

Kaikilla näillä kysymyksillä kuvataan heikon kohdan vakavuutta. Riski voidaan laskea yksinkertaisesti seuraavan kaavan avulla:

$$\text{Vaikutus} = \text{Riski} \times \text{mahdollinen vahinko}$$

Mahdollinen vahinko voi olla

- luvaton pääsy tietoihin
- palvelun esto (DOS)
- käyttövaltuutusten saanti tai laajentaminen

(Tämän luvun lopussa on esitetty tarkempia luokitusjärjestelmiä.)

Kun näihin kysymyksiin saadaan vastaukset, tiedotteeseen voidaan merkitä yleisarvio ja ilmoittaa mahdolliset riskit ja vahingot. Usein käytetään yksinkertaisia ilmaisuja, kuten ALHAINEN, KESKISUURI ja SUURI.

Muita kattavia riskinarviointijärjestelmiä ovat seuraavat:

GOVCERT.NL:n arviointijärjestelmä²¹

Alankomaiden hallituksen tietoturvaryhmä GOVCERT.NL on kehittänyt riskinarviointimatriisin. Matriisi kehitettiin Govcert.nl:n alkuvaiheessa, ja sitä päivitetään yhä viimeisimpien suuntausten mukaan.

RISK

Is the vulnerability widely known?	No, limited	1	Yes, public	2
Is the vulnerability widely exploited?	No	1	Yes	2
Is it easy to exploit the vulnerability?	No, hacker	1	Yes, script kiddie	2
Precondition: default configuration?	No, specific	1	Yes, standard	2
Precondition: physical access required?	Yes	1	No	2
Precondition: user account required?	Yes	1	No	2

11,12

High

8,9,10

Medium

0

6,7

Low

Damage

Unauthorized access to data	No	0	Yes, read	2	Yes, read +	4
DoS	No	0	Yes, non-critical	1	Yes, critica	5
Permissions	No	0	Yes, user	4	Yes, root	6

6 t/m 15

High

2 t/m 5

Medium

0

0,1

Low

OVERALL

High	Remote root	>> Immediately action needed!
	Local root exploit (attacker has a user account on the machine)	
Medium	Denial of Service	
	Remote user exploit	>> Action within a week
	Remote unauthorized access to data	
	Unauthorized obtaining data	
Low	Local unauthorized access to data	
	Local unauthorized obtaining user-rights	>> Include it in general process
	Local user exploit	

Kuva 11: GOVCERT.NL:n arviointijärjestelmä

EISPP:n tiedotteissa sovellettava malli²²

Euroopan tietoturvan edistämisen ohjelma (European Information Security Promotion Programme, EISPP) on Euroopan yhteisön viidennestä puiteohjelmasta yhteisrahoittama hanke. EISPP-hankkeen avulla pyritään ottamaan käyttöön eurooppalainen järjestelmä, jonka puitteissa jaetaan turvallisuustietoa ja määritetään pienille ja keskisuurille yrityksille jaettavien turvallisuustietojen sisältö ja jakelutavat. Antamalla eurooppalaisille pk-yrityksille tarvittavat tietoturvapalvelut niitä kannustetaan luottamaan sähköiseen kaupankäyntiin ja hyödyntämään sitä, mikä lisää ja parantaa uusien liiketoimien mahdollisuuksia. Euroopan komission tavoitteena on muodostaa eurooppalainen asiantuntijaverkko Euroopan unioniin, ja EISPP on sen edelläkävijä.

DAF Deutsches Advisory Format²³

DAF on Saksan CERT-Verbundin aloite. Sillä on keskeinen asema infrastruktuurissa, jossa eri ryhmät laativat tietoturvatiedotteita ja vaihtavat niitä. DAF on räätälöity erityisesti saksalaisten CERT-ryhmien tarpeisiin. CERT-Bund, DFN-CERT, PRESECURE ja Siemens-CERT kehittävät ja ylläpitävät tätä standardia.

²¹ Haavoittuvuusmatriisi: <http://www.govcert.nl/download.html?f=33>

²² EISPP: 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**Vaihe 3: Tiedon jakaminen**

CSIRT-ryhmä voi valita tiedon jakamistavan eri vaihtoehtoista asiakkaiden toiveiden ja viestintästrategian mukaan.

- Internet-sivut
- Sähköposti
- Raportit
- Arkistot ja tutkimus

CSIRT-ryhmän jakamissa tietoturvatiedotteissa olisi noudatettava samaa rakennetta. Näin parannetaan luettavuutta, ja lukija löytää nopeasti kaiken merkityksellisen tiedon.

Tiedotteessa on oltava vähintään seuraavat tiedot:

Tiedotteen otsikko
Viitenumero Järjestelmät, joita heikkous koskee - - Käyttöjärjestelmä ja käyttöjärjestelmän versio Riski (suuri–keskisuuri–alhainen) Vaikutus / mahdollinen vahinko (suuri–keskisuuri–alhainen) Ulkoiset tunnisteen: (CVE, heikkoutta koskevan tiedotteen tunnisteen)
Heikkouden arviointi Vaikutus Ratkaisu Kuvaus (yksityiskohdat) Liite

Kuva 12: Esimerkki tiedotemallista

Katso luku 10 ”Käytännön harjoitus: tietoturvatiedotteen laatiminen”.

Tietoturvaloukkausten käsittely

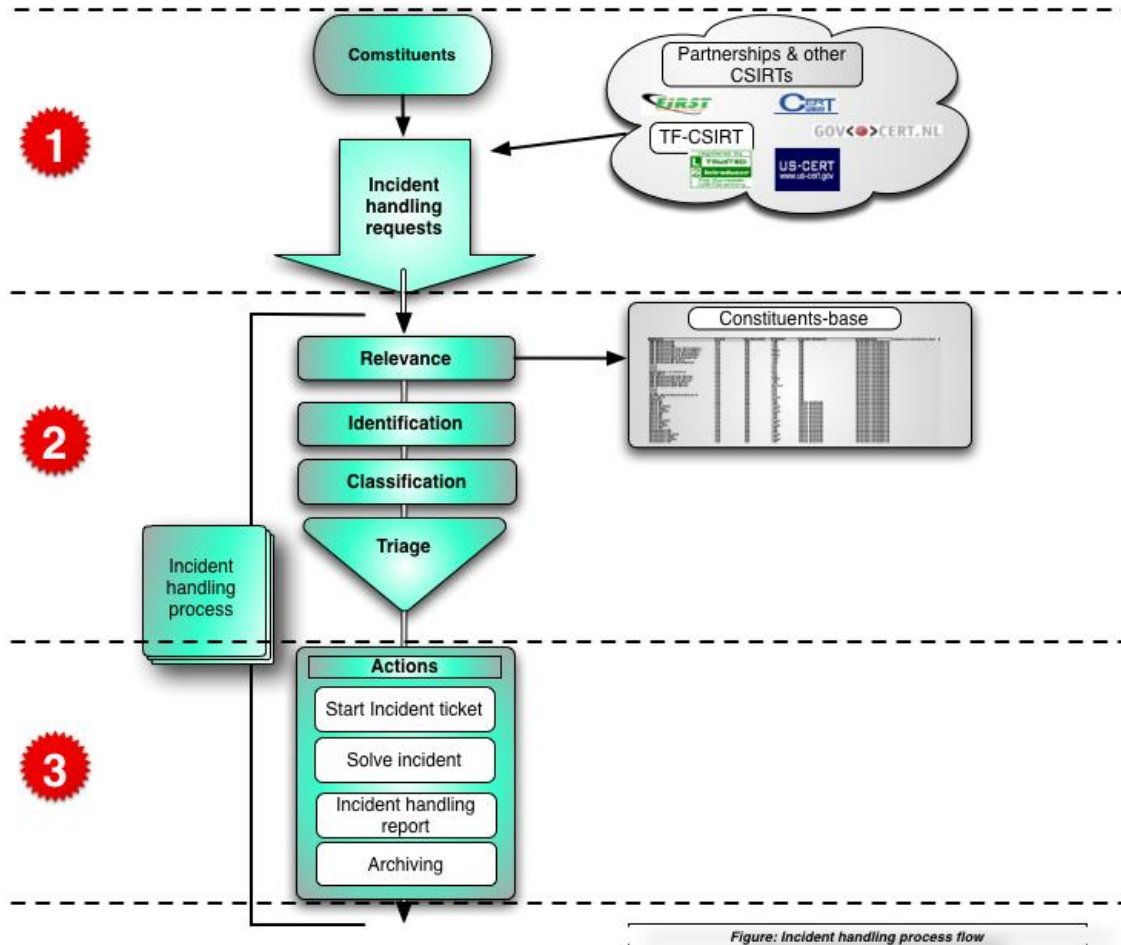
Kuten tämän luvun johdannossa todettiin, tietojen käsittelyn prosessi tietoturvaloukkausten käsittelyssä on hyvin samantapainen kuin hälytysten, varoitusten ja tiedotteiden laatimisen yhteydessä käytettävä menetelmä. Tiedonkeruuvaihe on kuitenkin yleensä erilainen, sillä tietoturvaloukkauksiin liittyvää tietoa saadaan tavallisesti asiakkaiden tai muiden ryhmien laatimien tietoturvaloukkauksia koskevien raporttien tai tietoturvaloukkausten käsittelyyn osallistuneiden tahojen antaman palautteen pohjalta. Tietoa vastaanotetaan sähköpostitse (salattu), ja joskus puhelimen tai faksin käyttö on välttämätöntä.

Kun tietoa vastaanotetaan puhelimitse, on hyvä merkitä heti muistiin jokainen yksityiskohta joko käyttämällä tietoturvaloukkausten käsittelyn/raportoinnin työkalua tai kirjoittamalla muistio. On välttämätöntä luoda heti (ennen puhelun päättymistä) tietoturvaloukkausnumero (jos kyseisellä tietoturvaloukkauksella ei tällaista vielä ole) ja antaa se raportijalle puhelimitse (tai lähettää myöhemmin yhteenveto sähköpostitse), jotta hän voi käyttää sitä vastedes viitteenä.

Tämän luvun loppuosassa kuvataan tietoturvaloukkausten käsittelyn perusprosessia. Perusteellinen analyysi tietoturvaloukkausten koko käsittelyprosessista ja siihen liittyvistä työnkuluista on esitetty CERT/CC-ryhmän asiakirjassa *"Defining Incident Management processes for CSIRTs"*.²⁴

²⁴ Tietoturvaloukkausten käsittelyprosessin määrittäminen: <http://www.cert.org/archive/pdf/04tr015.pdf>

Tietoturvaloukkausten käsittelyssä työnkulku on olennaisilta osin seuraava:



Kuva 13: Tietoturvaloukkausten käsittelyn kulku

1**Vaihe 1: Tietoturvaloukkauksia koskevien raporttien vastaanottaminen**

Kuten aikaisemmin todettiin, CSIRT-ryhmä saa tietoturvaloukkauksia koskevia raportteja eri kanavien välityksellä, lähinnä sähköpostitse mutta myös puhelimitse tai faksitse.

Kuten edellä mainittiin, tietoturvaloukkausraportin vastaanottamisen yhteydessä on suositeltavaa kirjata kaikki yksityiskohdat vakiolomakkeeseen. Näin varmistetaan, ettei mitään oleellista tietoa jää pois. Jäljempänä esitetään mallilomake:

TIETOTURVALOUKKAUSTEN RAPORTOINTILOMAKE

*Täytetty lomake lähetetään faksitse tai sähköpostitse seuraavaan osoitteeseen:
Tiedot, jotka on merkitty tähdellä (*), ovat pakollisia.*

Nimi ja organisaatio

1. Nimi*:
2. Organisaation nimi*:
3. Toimiala:
4. Maa*:
5. Kaupunki:
6. Sähköpostiosoite*:
7. Puhelinnumero*:
8. Muu:

Toimeksiantaja/toimeksiantajat, jota/joita tietoturvaloukkaus koskee

9. Toimeksiantajien määrä:
10. Toimeksiantajan nimi ja IP-osoite*:
11. Toimeksiantajan tehtävä*:
12. Aikavyöhyke:
13. Laitteisto:
14. Käyttöjärjestelmä:
15. Ohjelmisto, jota tietoturvaloukkaus koskee:
16. Tiedostot, joita tietoturvaloukkaus koskee:
17. Turvallisuus:
18. Toimeksiantajan nimi ja IP:
19. Yhteyskäytäntö/portti:

Tietoturvaloukkaus

20. Viitenumero ref #:
21. Tietoturvaloukkauksen tyyppi:
22. Tietoturvaloukkauksen alkamisajankohta:
23. Onko kyse jatkuvasta tietoturvaloukkauksesta: Kyllä (YES) Ei (NO)
24. Tunnistettu (kellonaika ja menetelmä):
25. Tunnetut heikot kohdat:
26. Epäilyttävät tiedostot:
27. Torjuntatoimet:
28. Yksityiskohtainen kuvaus*:

Kuva 14: Tietoturvaloukkausta koskevan raportin sisältö

Vaihe 2: Tietoturvaloukkauksen arviointi



Tässä vaiheessa tarkistetaan ilmoitetun tietoturvaloukkauksen aitous ja merkityksellisyys ja luokitellaan tietoturvaloukkauksen vakavuus.

Tunnistaminen

Tarpeettomien toimien estämiseksi on hyvä tarkistaa, onko lähettäjä luotettava ja kuuluuko lähettäjä oman CSIRT-ryhmän tai toisen CSIRT-ryhmän asiakkaisiin. Sovellettavat säännöt ovat samat kuin luvussa 8.2 ”Hälytysten tuottaminen”.

Merkityksellisyys

Tässä vaiheessa tarkistetaan, onko tietoturvaloukkauksen käsittelypyyntö peräisin CSIRT:n asiakaskunnalta tai kuuluvatko asiakaskunnan tietotekniikkajärjestelmät ilmoitetun tietoturvaloukkauksen piiriin. Jos kyse ei ole kummastakaan, raportti yleensä reititetään uudelleen oikealle CSIRT-ryhmälle.²⁵

Luokitus

Tässä vaiheessa tietoturvaloukkaukset luokitellaan niiden vakavuuden mukaan (triage). Tässä asiakirjassa ei käsitellä tietoturvaloukkausten luokituksen yksityiskohtia. CSIRT-ryhmän luokitusjärjestelmä tarjoaa hyvän lähtökohdan (esimerkiksi yrityksen CSIRT-ryhmälle):

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.

Kuva 15: Tietoturvaloukkausten luokitusjärjestelmä (lähde: FIRST)²⁶

²⁵ Työkalut identiteetin tarkistamiseksi CHIHT:ssä: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

²⁶ CSIRT:n tapausluokitus http://www.first.org/resources/guides/csirt_case_classification.html

Triage (luokittelu)

Triage on terveydenhoito- tai hälytys henkilöstön käyttämä luokittelujärjestelmä, jolla säännöstellään vähäisiä lääkintäresursseja, kun hoitoa tarvitsevien loukkaantuneiden määrä ylittää käytettävät resurssit, jotta mahdollisimman moni potilas saisi hoitoa.²⁷

CERT/CC-ryhmän antama kuvaus on seuraava:

Triage on olennainen osa tietoturvaloukkauksen käsittelyä, varsinkin vakiintuneessa CSIRT-ryhmässä. Triage-luokittelua tarvitaan, jotta koko organisaatio ymmärtää, mistä raportoinnissa on kyse. Se toimii välineenä, jonka kautta kaikki tieto virtaa yhteen yhteyspisteeseen, jolloin voidaan saada yrityksenlaajuinen käsitys käynnissä olevista toimista ja järjestää kaikki ilmoitetut tiedot kokonaisvaltaisesti. Triage mahdollistaa vastaanotetun raportin alustavan arvioinnin ja asettaa sen jonoon jatkokäsittelyä varten. Se antaa myös mahdollisuuden aloittaa alustavan dokumentoinnin ja raporttia tai pyyntöä koskevien tietojen tallentamisen, jos tätä ei ole vielä tehty tunnistusmenettelyssä.

Triage-toiminnolla saadaan nopea kuva ilmoitettujen toimien nykytilasta, toisin sanoen siitä, minkä raporttien käsittely on vielä kesken ja mitkä on saatettu päätökseen, mitkä toimet ovat vireillä ja kuinka monta kunkin tyyppistä raporttia on vastaanotettu. Tämä prosessi voi auttaa tunnistamaan mahdolliset turvallisuusongelmat ja priorisoimaan työtaakkaa. Triage-luokittelun aikana kerättyjä tietoja voidaan myös käyttää heikkoihin kohtiin ja tietoturvaloukkauksiin liittyvien suuntauksien ja tilastojen laatimiseen ylemmälle johdolle.²⁸

Ainoastaan ryhmän kokeneimpien jäsenten pitäisi tehdä triage-luokittelua, sillä se edellyttää tietoturvaloukkauksista asiakaskunnalle mahdollisesti aiheutuvien vaikutusten laajamittaista ymmärtämistä ja kykyä päättää, kuka on sopiva henkilö käsittelemään kyseistä tietoturvaloukkausta.

²⁷ Triage Wikipediassa: <http://en.wikipedia.org/wiki/Triage>.

²⁸ Tietoturvaloukkausten käsittelymenettelyn määrittely: <http://www.cert.org/archive/pdf/04tr015.pdf>.

Vaihe 3: Toimenpiteet

Luokitellut loukkaukset laitetaan yleensä pyyntöjonoon tietoturvaloukkauksia käsittelevään työkaluun. Sitä käyttää yksi tai useampi käsittelijä, jotka periaatteessa noudattavat seuraavia vaiheita:

Tietoturvaloukkaustiketin luominen

Tietoturvaloukkauksen tikettinumero on ehkä jo luotu edellisessä vaiheessa (esim. kun loukkauksesta ilmoitettiin puhelimitse). Jos ei, ensimmäiseksi on luotava numero, jota käytetään jatkossa tämän tietoturvaloukkauksen käsittelyn yhteydessä.

Tietoturvaloukkauksen elinkaari

Tapahtumaa käsiteltäessä eri vaiheet eivät seuraa toisiaan peräkkäin siten, että lopulta päädytään ratkaisuun, vaan eri vaiheet etenevät pikemminkin sykleittäin siten, että vaiheita sovelletaan yhä uudelleen, kunnes tietoturvaloukkaus on lopulta ratkaistu ja kaikilla osapuolilla on kaikki tarvittavat tiedot. Tämä sykli, jota kutsutaan usein "tietoturvaloukkausten elinkaareksi", sisältää seuraavat prosessit:

<i>Analysointi:</i>	Kaikki ilmoitettua tietoturvaloukkausta koskevat tiedot analysoidaan.
<i>Yhteystietojen haku:</i>	Tietoturvaloukkaukseen liittyvät tiedot voidaan siten ilmoittaa kaikille osapuolille, kuten muille CSIRT-ryhmille, tietoturvaloukkauksen kohteille ja luultavasti hyökkäykseen mahdollisesti käytettyjen järjestelmien omistajille.
<i>Teknisen tuen tarjoaminen:</i>	Autetaan tietoturvaloukkauksen kohteita toipumaan tietoturvaloukkauksen seurauksista ja keräämään lisätietoa hyökkäyksestä.
<i>Koordinointi:</i>	Tiedotetaan tapahtumista muille asianosaisille, kuten hyökkäyksessä käytetystä IT-järjestelmästä vastaavalle CSIRT-ryhmälle tai muille tietoturvaloukkauksen kohteille.

Tätä rakennetta kutsutaan "elinkaareksi", koska yksi vaihe johtaa toiseen ja viimeinen vaihe, koordinointi, voi puolestaan johtaa uuteen analyysiin, ja sykli alkaa jälleen. Prosessi päättyy, kun kaikki osapuolet ovat saaneet ja ilmoittaneet kaikki tarvittavat tiedot.

Tietoturvaloukkausten elinkaarta on kuvattu yksityiskohtaisemmin CERT/CC:n CSIRT-käsikirjassa.²⁹

Raportti tietoturvaloukkauksen käsittelystä

Valmistaudu vastaamaan johdon kysymyksiin tietoturvaloukkauksesta laatimalla raportti. Kokemuksista on hyvä laatia asiakirja (ainoastaan sisäiseen käyttöön), jota käytetään henkilöstön kouluttamisessa ja virheiden välttämiseksi tulevilla tietoturvaloukkausten käsittelyn prosesseissa.

²⁹ CSIRT-käsikirja: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>.

Arkistointi

Katso arkistointia koskevat säännöt, jotka on esitetty edellä luvussa 6.6 ”Tietoturvapoliitikan laatiminen”.

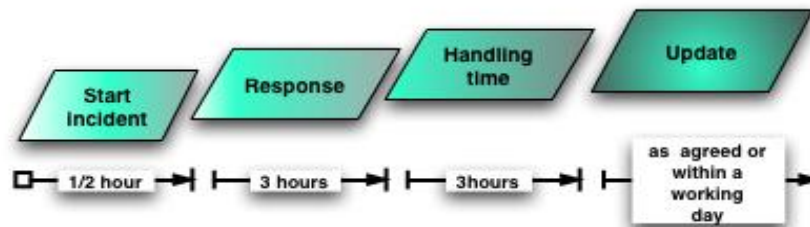
Lisätietoa tietoturvaloukkausten käsittelystä ja tietoturvaloukkausten elinkaaresta on liitteen osassa A.1 Lisälukemista.

Esimerkki käsittelyaikataulusta

Käsittelyaikataulu jätetään usein vahvistamatta, mutta sen on sisällyttävä kaikkiin hyvin laadittuihin CSIRT-ryhmän ja asiakaskunnan väliin palvelutasosopimukseen (SLA). Oikea-aikaisen palautteen antaminen asiakkaille tietoturvaloukkausten käsittelyn aikana on olennaisen tärkeää sekä asiakkaiden oman vastuun että ryhmän maineen takia.

Käsittelyajat on ilmoitettava asiakkaille selkeästi väärin odotusten välttämiseksi. Seuraavaa perusaikataulua voidaan käyttää CSIRT:n ja asiakaskunnan välisen yksityiskohtaisemman SLA-sopimuksen lähtökohtana.

Jäljempänä on esimerkki käytännön käsittelyn aikataulusta alkaen apua koskevan pyynnön vastaanottamisesta:



Kuva 16: Esimerkki käsittelyaikataulusta

On hyvän käytännön mukaista antaa asiakaskunnalle ohjeet sen omista reagointiajoista ja etenkin siitä, milloin sen on otettava yhteyttä CSIRT-ryhmään hätätapauksissa. Useimmiten on järkevää ottaa yhteyttä CSIRT-ryhmään jo aikaisessa vaiheessa. On suositeltavaa rohkaista asiakkaita ottamaan yhteyttä, jos he ovat epävarmoja asiasta.

Käytettävissä olevat CSIRT-työkalut

Tässä luvussa viitataan CSIRT-ryhmien käyttämiin yleisiin työkaluihin. Tässä yhteydessä annetaan vain esimerkkejä, lisää viittauksia on annettu asiakirjassa *Clearinghouse of Incident Handling Tools* -sivuilla (CHIHT).³⁰

Sähköpostin ja viestien salausohjelmisto

- GnuPG <http://www.gnupg.org/>
GnuPG on GNU-hankkeen kattava ja maksuton OpenPGP-standardia (RFC2440) tukeva ohjelmisto. GnuPG-ohjelmistoa voidaan käyttää tietojen ja viestien salaukseen ja allekirjoittamiseen.
- PGP <http://www.pgp.com/>
Kaupallinen versio

Tietoturvaloukkausten käsittelyn työkalut

Tietoturvaloukkausten hoito ja niiden jatkokäsittely, toimien seuranta.

- RTIR <http://www.bestpractical.com/rtir/>
RTIR on maksuton, avoimeen lähdekoodiin perustuva tietoturvaloukkausten käsittelyjärjestelmä, joka on suunniteltu ottaen huomioon CERT-ryhmien ja muiden tietoturvaloukkauksia käsittelevien ryhmien tarpeet.

CRM-työkalut

CRM-tietokannasta on hyötyä, jos erilaisia asiakkaita on hyvin paljon ja kaikkia tapaamisia ja yksityiskohtia on seurattava tarkasti. Siitä on monia erilaisia variantteja, jäljempänä on esitetty joitakin esimerkkejä:

- SugarCRM <http://www.sugarcrm.com/crm/>
- Sugarforce
(maksuton avoimeen lähdekoodiin perustuva versio) <http://www.sugarforge.org/>

Tietojen tarkistus

- Website watcher <http://www.aignes.com/index.htm>
Ohjelma seuraa verkkosivujen päivityksiä ja muutoksia.
- Watch that page <http://www.watchthatpage.com/>
Palvelu lähettää tietoa verkkosivujen muutoksista sähköpostitse (maksuton ja kaupallinen).

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

Yhteystietojen löytäminen

Ei ole helppoa löytää oikeaa yhteyshenkilöä, jolle voi ilmoittaa tietoturvaloukkauksista. Jäljempänä on mainittu joitakin tietolähteitä, joita voi käyttää:

- RIPE³¹
- IRT-objekti³²
- TI³³

Lisäksi CHIHT on luetellut joitakin työkaluja, joita voi käyttää yhteystietojen löytämiseen.³⁴

Kuvitteellinen CSIRT (vaihe 8)

Työnkulkujen ja toiminnallisten ja teknisten menettelyjen vahvistaminen

Keskeiset kuvitteellisen CSIRT-ryhmän tarjoamat palvelut ovat seuraavat:

- Hälytykset ja varoitukset
- Tiedotteet
- Tietoturvaloukkausten käsittely

Ryhmä on kehittänyt toimivia menettelyjä, joita ryhmän kaikkien jäsenten on helppo ymmärtää. Kuvitteellinen CSIRT-ryhmä rekrytoi myös oikeudellisen asiantuntijan, joka tarkastelee vastuukysymyksiä ja tietoturvapoliittikkaa. Ryhmä on kehittänyt myös hyödyllisiä työkaluja ja saanut hyödyllistä tietoa toiminnallisista kysymyksistä keskustelemalla muiden CSIRT-ryhmien kanssa.

Tietoturvatiedotteita ja tietoturvaloukkauksia koskevia raportteja varten on laadittu vakiomalli. Ryhmä käyttää RTIR-järjestelmää (Request Tracker for Incident Response) tietoturvaloukkausten käsittelemiseen.

³¹ RIPE whois: <http://www.ripe.net/whois>

³² IRT-objekti RIPE-tietokannassa: 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 Työkalut identiteetin tarkistamiseksi CHIHT:ssä: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 CSIRT-koulutus

Tähän mennessä on toteutettu seuraavat vaiheet:

1. Mikä on CSIRT on ja mitä hyötyä siitä on?
2. Mille toimialalle uusi ryhmä tarjoaa palveluja?
3. Mitä palveluja CSIRT-ryhmä voi tarjota asiakaskunnalleen
4. Toimintaympäristön ja asiakkaiden arviointi
5. Toimenkuvan määrittäminen
6. Liiketoimintasuunnitelman laatiminen
 - a. Rahoitusmallin määrittäminen
 - b. Organisaatorakenteen määrittäminen
 - c. Henkilöstön rekrytoinnin aloittaminen
 - d. Toimiston käyttö ja laitteistot
 - e. Tietoturvapoliittikan laatiminen
 - f. Yhteistyökumppaneiden etsiminen
7. Liiketoimintasuunnitelman edistäminen
 - a. Liiketoimintasuunnitelman hyväksyttäminen
 - b. Eri osien sisällyttäminen hankesuunnitelmaan
8. CSIRT-ryhmän suorituskyvyn varmistaminen
 - a. Työnkulkujen laatiminen
 - b. CSIRT-työkalujen käyttöönotto

>> Seuraava vaihe on henkilöstön koulutus

Tässä luvussa tarkastellaan kahta tärkeintä tahoa, jotka tarjoavat CSIRT-koulutusta: TRANSITS ja CERT/CC.

TRANSITS

TRANSITS (Training of Network Security Incident Teams Staff) on eurooppalainen hanke, jolla edistetään tietoturvaryhmien (CSIRT) perustamista ja jo toiminnassa olevien CSIRT-ryhmien toimintaa. Hankkeella pyritään poistamaan ammattitaitoisen CSIRT-henkilöstön puutteen ongelma. Tämän tavoitteen saavuttamiseksi on järjestetty erityisiä koulutuskursseja (uusien) CSIRT-ryhmien henkilöstön kouluttamiseksi CSIRT-palvelujen tarjoamiseen liittyvissä organisaatiota, toimintaa, tekniikkaa, markkinoita ja oikeutta koskeissa kysymyksissä.

TRANSITS-hankkeessa on etenkin

- kehitetty, päivitetty ja tarkistettu säännöllisesti moduuleista muodostuvaa kurssimateriaalia
- järjestetty koulutustyöpajoja, joissa on jaettu kurssimateriaalia
- otettu uusien CSIRT-ryhmien, erityisesti liittymisneuvotteluja käyvien maiden CSIRT-ryhmien, henkilöstöä mukaan näihin koulutustyöpajoihin,
- jaettu kurssimateriaalia ja varmistettu tulosten hyödyntäminen.³⁵

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

ENISA edistää ja tukee TRANSITS-kursseja. Kurseille hakemisesta, vaatimuksista ja kustannuksista antavat lisätietoja ENISAn CSIRT-asiantuntijat:

CERT-Relations@enisa.europa.eu

Tämän asiakirjan liitteessä on esitetty esimerkkejä kurssimateriaalista.

CERT/CC

Tieto- ja verkkoinfrastruktuurien monimutkaisuuden ja hallinnollisten haasteiden takia on vaikeaa varmistaa verkon asianmukainen suojaus. Verkon ja järjestelmän ylläpitäjillä ei ole käytettävissään tarpeeksi henkilökuntaa tai riittäviä turvatoimia, jotta ne voisivat torjua hyökkäykset ja minimoida vahingot. Tämän seurauksena tietoturvaloukkausten määrä kasvaa.

Kun tietoturvaloukkauksia tapahtuu, organisaatioiden on reagoitava nopeasti ja tehokkaasti. Mitä nopeammin organisaatio tunnistaa ja analysoi tietoturvaloukkauksen ja reagoi siihen, sitä paremmin se voi vähentää vahinkoja ja vahingoista toipumisen kustannuksia. Tietoturvaloukkausten käsittelyryhmän (CSIRT) perustaminen on hyvä keino ottaa käyttöön nopean toiminnan voimavaroja ja auttaa estämään tulevia tietoturvaloukkauksia.

CERT-CC tarjoaa johtajille ja tekniselle henkilöstölle kursseja esimerkiksi tietoturvaloukkauksia käsittelevien ryhmien (CSIRT) perustamisessa ja johtamisessa, tietoturvaloukkausten käsittelyssä ja analysoinnissa sekä verkkoturvallisuuden parantamisessa. Jollei toisin ilmoiteta, kaikki kurssit pidetään Pittsburghissa (Pennsylvania). Henkilöstömme antaa myös tietoturvakoulutusta Carnegie Mellonin yliopistossa.

Erityisesti CSIRT-ryhmille tarkoitettut CERT/CC-kurssit³⁶

Tietoturvaloukkauksia käsittelevän ryhmän (CSIRT) perustaminen

Tietoturvaloukkauksia käsittelevän ryhmän johtaminen

Tietoturvaloukkausten käsittelyn perusteet

Tekniselle henkilöstölle tarkoitettu tietoturvaloukkausten tehostettu käsittely

Tämän asiakirjan liitteessä on esitetty esimerkkejä kurssimateriaalista.

Kuvitteellinen CSIRT-ryhmä (vaihe 9)

Henkilöstön koulutus

Kuvitteellinen CSIRT-ryhmä päättää lähettää teknisen henkilöstönsä seuraavaksi järjestettäville TRANSITS-kurseille. Ryhmän johtaja osallistuu myös CERT/CC-kurssille "CSIRT-ryhmän johtaminen".

³⁶ CERT/CC-kurssit: <http://www.sei.cmu.edu/products/courses>

10 Käytännön harjoitus: tietoturvatiedotteen laatiminen

Tähän mennessä on toteutettu seuraavat vaiheet:

1. Mikä on CSIRT on ja mitä hyötyä siitä on?
2. Mille toimialalle uusi ryhmä tarjoaa palveluja?
3. Mitä palveluja CSIRT-ryhmä voi tarjota asiakaskunnalleen
4. Toimintaympäristön ja asiakkaiden arviointi
5. Toimenkuvan määrittäminen
6. Liiketoimintasuunnitelman laatiminen
 - a. Rahoitusmallin määrittäminen
 - b. Organisaatorakenteen määrittäminen
 - c. Henkilöstön rekrytoinnin aloittaminen
 - d. Toimiston käyttö ja laitteistot
 - e. Tietoturvapoliittikan laatiminen
 - f. Yhteistyökumppaneiden etsiminen
7. Liiketoimintasuunnitelman edistäminen
 - a. Liiketoimintasuunnitelman hyväksyttäminen
 - b. Eri osien sisällyttäminen hankesuunnitelmaan
8. CSIRT-ryhmän suorituskyvyn varmistaminen
 - a. Työnkulkujen laatiminen
 - b. CSIRT-työkalujen käyttöönotto
9. Henkilöstön kouluttaminen

>> Seuraavassa vaiheessa tehdään harjoitustyö ja valmistaudutaan käytännön toimiin.

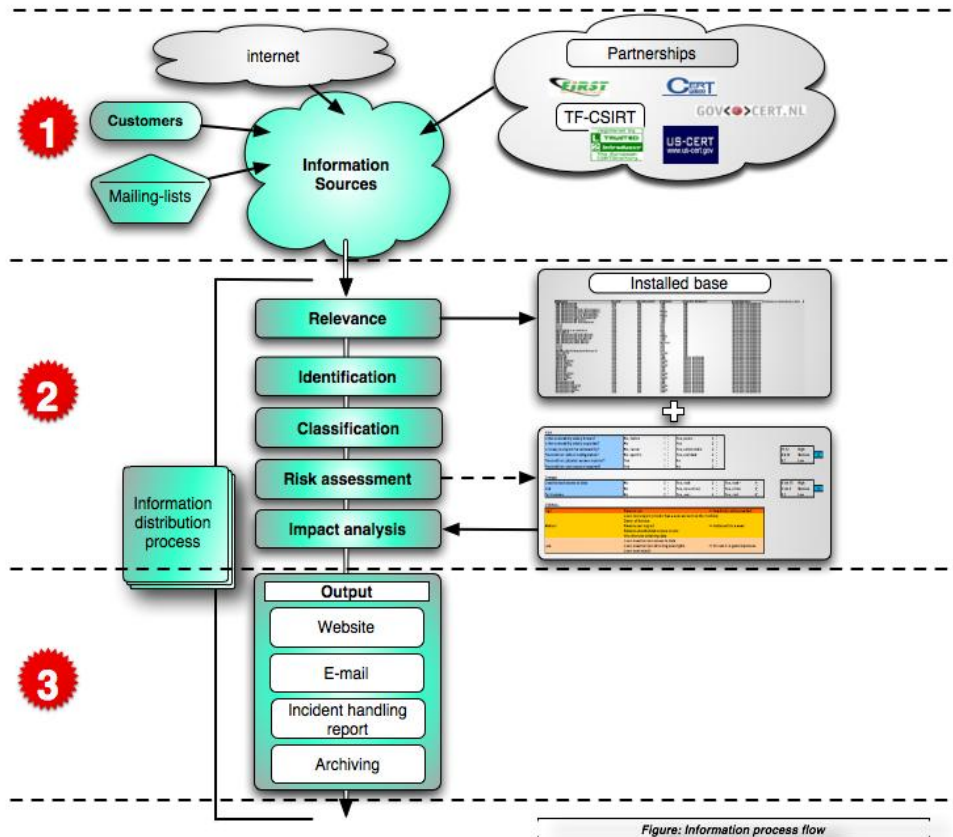
Tässä luvussa esitetään havainnollisesti eräs CSIRT:n päivittäisiin toimiin kuuluva tehtävä, nimittäin tietoturvatiedotteen laatiminen.

Vaikuttimena oli seuraava Microsoftin lähettämä alkuperäinen tietoturvatiedote:

Tiedotteen numero	Microsoftin tietoturvatiedote MS06-042
Tiedotteen otsikko	Internet Explorerin koottu tietoturvapäivitys (918899)
Yhteenvedo	Päivityksellä ratkaistaan useita Internet Explorerin heikkoja kohtia, jotka voivat mahdollistaa ohjelmakoodin purkamisen verkon välityksellä.
Haavoittuvuuden vakavuusaste	Kriittinen
Haavoittuvuuden vaikutus	Ohjelmakoodin purkaminen verkon välityksellä (Remote Code Execution)
Haavoittuvat ohjelmistot	Windows, Internet Explorer. Ks. lisätietoa kohdasta "Haavoittuvat ohjelmistot ja lataussijainti".

Tässä palveluntoimittajan tietoturvatiedotteessa käsitellään hiljattain todettua Internet Explorerin heikkoa kohtaa. Palveluntoimittaja julkaisee useita ohjelmistoa koskevia korjauksia Microsoft Windowsin eri versioita varten.

Saatuaan heikkoa kohtaa koskevan tiedon postituslistan kautta kuvitteellinen CSIRT käynnistää luvussa 8.2 "Hälytysten, varoitusten ja tiedotteiden tuottaminen" kuvatut toimet



1

Vaihe 1: Heikkoja kohtia koskevan tiedon kerääminen.

Ensimmäisessä vaiheessa kuvitteellinen CSIRT vierailee palveluntarjoajan verkkosivuilla ja todentaa tiedon aitouden sekä kerää yksityiskohtaisia tietoja heikosta kohdasta ja IT-järjestelmistä, joita se koskee.

2**Vaihe 2: Tietojen ja riskien arviointi****Tunnistaminen**

Tieto on jo varmennettu vertaamalla sähköpostissa saatua tietoa heikosta kohdasta palveluntarjoajan verkkosivuilla julkaisemaan tietoon.

Merkityksellisyys

Kuvitteellinen CSIRT vertaa verkkosivuilla julkaistua luetteloa ohjelmistoista, joita heikko kohta koskee, asiakaskunnan käyttämien järjestelmien luetteloon. Se toteaa, että ainakin yksi sen asiakkaista käyttää Internet Exploreria, joten heikkoa kohtaa koskeva tieto on merkityksellinen.

Luokka	Sovellus	Ohjelmisto	Versio	Käyttö-järjestelmä	Versio	Asiakas
Sovellus	Selain	IE	x-x-	Microsoft	XP-prof.	A

Luottamuksellisuus

Tieto on julkista, joten sitä voidaan käyttää ja jakaa eteenpäin.

Riskien ja vaikutusten arviointi

Vastaamalla kysymyksiin todetaan, että riskit ja vaikutukset ovat *suuret* (Microsoftin luokituksen mukaan *kriittisiä*).

RISKIT

Tunnetaanko heikko kohta yleisesti?	K (Y)
Onko heikkous levinnyt laajalle?	K (Y)
Onko heikkoa kohtaa helppo käyttää hyväksi?	K (Y)
Voidaanko heikkoa kohtaa käyttää hyväksi etäältä?	K (Y)

VAHINGOT

Mahdollisia vaikutuksia ovat etäkäyttö ja mahdollisesti etäyhteydellä tapahtuva ohjelmakoodin suorittaminen (remote code execution). Tämä heikko kohta sisältää useita riskejä, minkä takia riski on *suuri*.



Vaihe 3: Jakelu

Kuvitteellinen CSIRT on yrityksen sisäinen tietoturvaryhmä. Sillä on käytössään viestintäkanavina sähköposti, puhelin ja sisäinen verkkosivusto. CSIRT-yksikkö laatii tiedotteen luvussa 8.2 *"Hälytysten, varoitusten ja tiedotteiden tuottaminen"* esitetyn mallin pohjalta.

Tiedotteen otsikko Internet Explorerissa havaittu useita heikkoja kohtia	
Viitenumero 082006-1	
Järjestelmät, joita heikko kohta koskee Kaikki sovellusjärjestelmät, joissa käytetään Microsoftia	
Käyttöjärjestelmä ja käyttöjärjestelmän versio - Microsoft Windows 2000 Service Pack 4 - Microsoft Windows XP Service Pack 1 ja Microsoft Windows XP Service Pack 2 - Microsoft Windows XP Professional x64 Edition - Microsoft Windows Server 2003 ja Microsoft Windows Server 2003 Service Pack 1 - Microsoft Windows Server 2003 Itanium-pohjaisissa järjestelmissä ja Microsoft Windows Server 2003, SP1 Itanium-pohjaisissa järjestelmissä - Microsoft Windows Server 2003 x64 Edition	
Riski SUURI	(suuri–keskisuuri–vähäinen)
Vaikutus/mahdolliset vahingot SUURI	(suuri–keskisuuri–vähäinen)
Ulkoinen tunnus: MS-06-42	(CVE, heikkoa kohtaa koskevan tietoturvatiedotteen tunnus)
Heikkoa kohtaa koskeva tiivistelmä Microsoft on löytänyt Internet Explorerissa useita kriittisiä heikkoja kohtia, jotka voivat johtaa ohjelmakoodin suorittamiseen verkon välityksellä.	
Vaikutus Hyökkääjä voi ottaa hallintaansa koko järjestelmän, asentaa ohjelmia, lisätä käyttäjiä ja katsella, muuttaa tai poistaa tietoja. Lieventävä seikka on se, että edellä kuvatut toimet ovat mahdollisia vain, jos käyttäjä on kirjautunut järjestelmään ylläpitäjän oikeuksilla. Vaikutukset voivat olla lievempiä niiden käyttäjien osalta, joilla on suppeammat käyttöoikeudet.	
Ratkaisu Tehdään välittömästi korjaukset Internet Explorer -selainohjelmaan.	
Kuvaus (yksityiskohdat) Ks. lisätietoa osoitteesta ms06-042.msp	

Liite

Ks. lisätietoa osoitteesta [ms06-042.msp](#)

Tämä tiedote voidaan nyt laittaa jakeluun. Koska kyse on kriittisestä tiedotteesta, on suositeltavaa, että asiakkaille tiedotetaan mahdollisuuksien mukaan myös puhelimitse.

Kuvitteellinen CSIRT (vaihe 10)**Käytännön harjoitus**

Ensimmäisten toimintaviikkojen aikana kuvitteellinen CSIRT-ryhmä käyttää käytännön harjoituksen pohjana useita (muilta CSIRT-ryhmiltä saamia) kuvitteellisia tapauksia. Lisäksi julkaistaan muutamia tietoturvatiedotteita laitteisto- ja ohjelmistotarjoajien jakamien todellisten heikkoja kohtia koskevien tietojen pohjalta, kun niitä on ensin hienosäädetty ja mukautettu asiakaskunnan tarpeisiin.

11 Päätelmät

Opas päättyy tähän. Tässä asiakirjassa esitetään hyvin suppea katsaus CSIRT-ryhmän perustamisen eri menettelyihin. Oppaan ei ole tarkoitus olla tyhjentävä, eikä siinä anneta yksityiskohtaista tietoa. Lisätietoa aihetta koskevasta kirjallisuudesta on kohdassa *A.1 Lisälukemista*.

Kuvitteellisen CSIRT-ryhmän seuraavat tärkeät vaiheet olisivat:

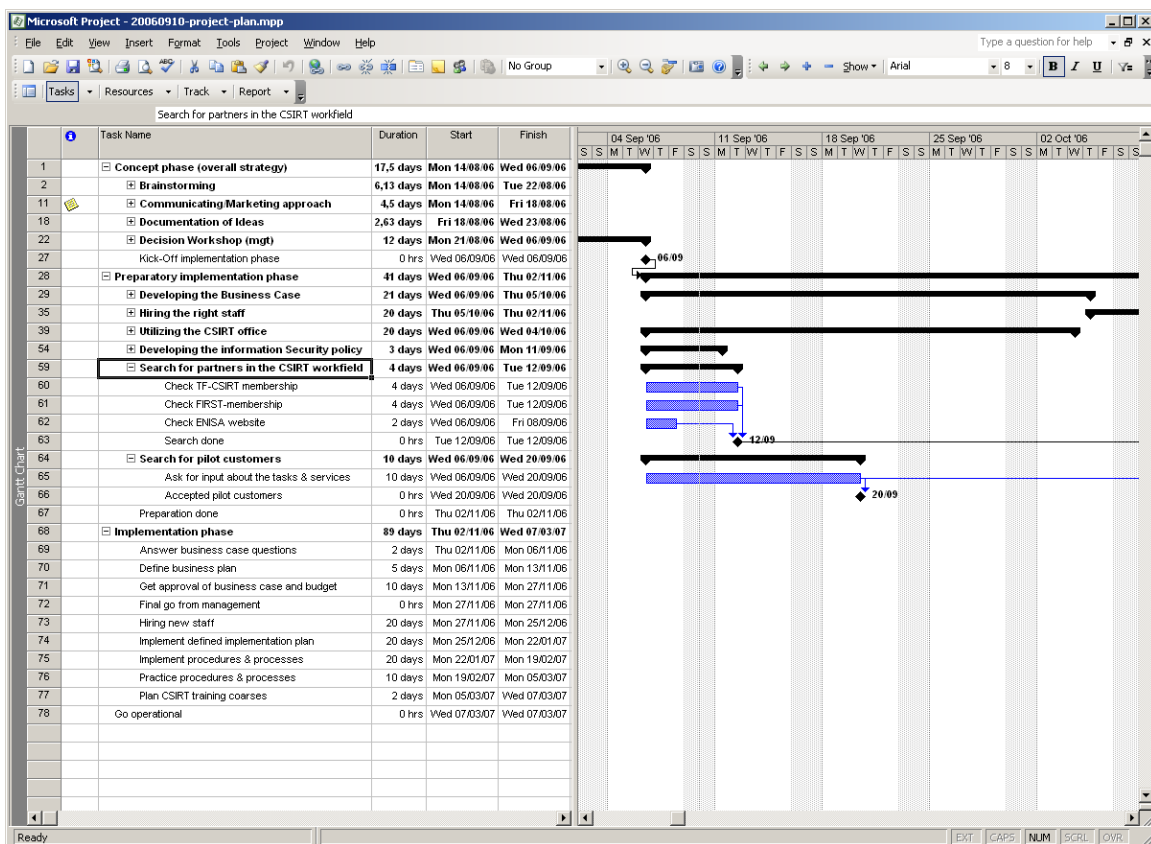
- Palautteen saaminen asiakaskunnalta tarjottavien palvelujen hienosäätämiseksi.
- Rutiinin hankkiminen päivittäiseen työhön.
- Häätötilanteiden harjoittelu.
- Tiiviin yhteistyön tekeminen eri CSIRT-yhteisöjen kanssa ja osallistuminen niiden vapaaehtoistyöhön yhden päivän ajan.

12 Hankesuunnitelman kuvaus

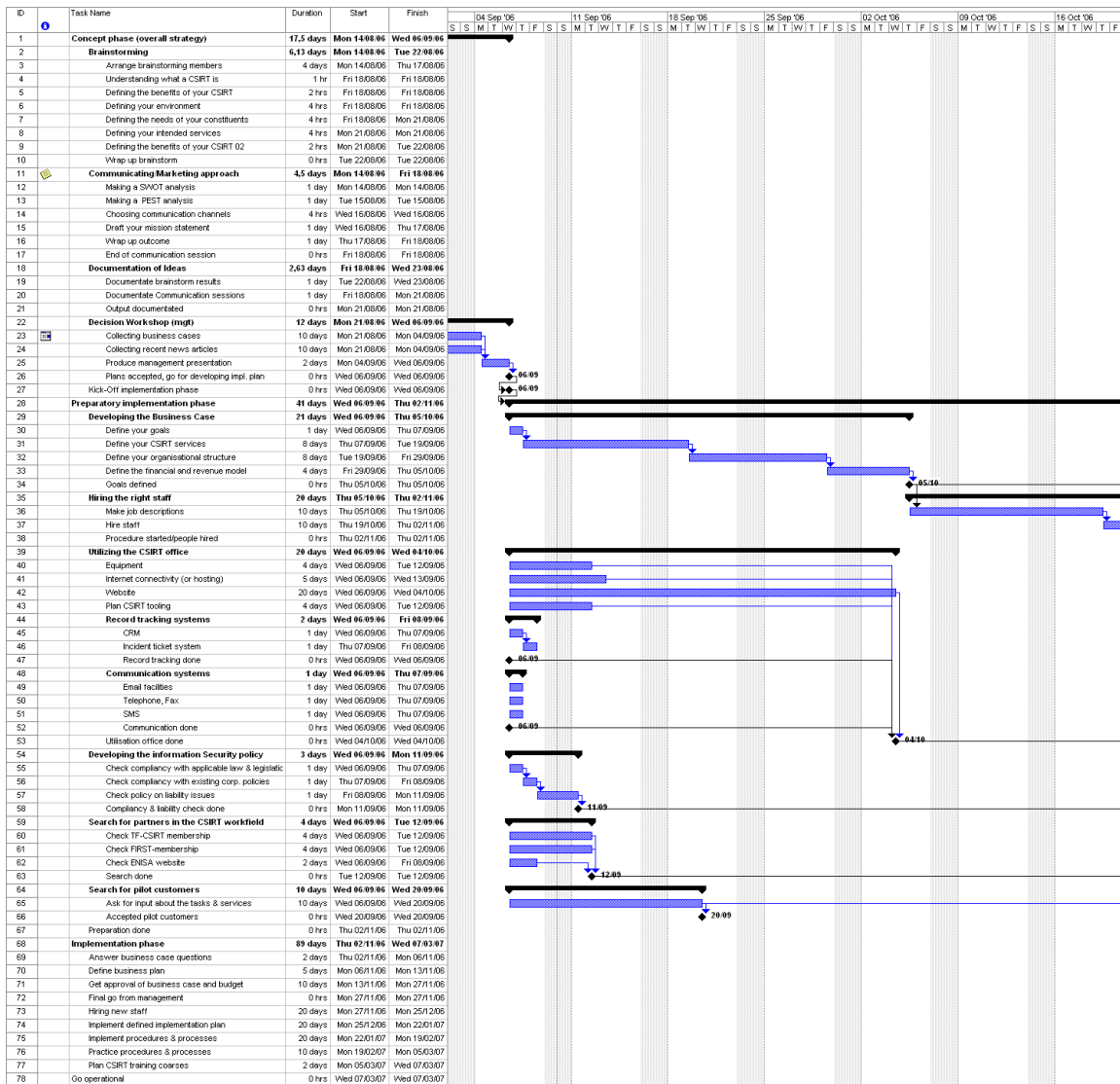
HUOMAUTUS: Hankesuunnitelma on ensimmäinen arvio tarvittavasta ajasta. Käytettävissä olevista resursseista riippuen hankkeen todellinen kesto voi erota suunnitellusta.

Hankesuunnitelma on saatavana eri muodoissa CD-levyllä ja ENISAn verkkosivuilta. Se kattaa kaikki tässä asiakirjassa kuvatut menettelyt.

Ensisijainen muoto on Microsoft Project, joten sitä voidaan käyttää suoraan tässä hankkeen johtamisen työkalussa.



Kuva 17: Hankesuunnitelma



Kuva 18: Hankesuunnitelma kaikkine tehtävineen ja osa Gant-kaaviosta

Hankesuunnitelma on saatavana myös CVS- ja XML-muodossa. Kysymyksiä sen käytöstä voi esittää ENISAn CSIRT-asiantuntijoille: CERT-Relations@enisa.europa.eu

LIITE

A.1 Lisälukemista

Handbook for CSIRTs (CERT/CC)

Kattava hakuteos, joka sisältää kaikki CSIRT-ryhmän työhön liittyvät aiheet.

Lähde: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

Defining Incident Management Processes for CSIRTs: A Work in Progress

Tietoturvaloukkausten käsittelyn perusteellinen analyysi.

Lähde: <http://www.cert.org/archive/pdf/04tr015.pdf>

State of the Practice of Computer Security Incident Response Teams (CSIRTs)

Kattava analyysi maailmanlaajuisen CSIRT-ympäristön tilanteesta, myös historia, tilastot jne.

Lähde: <http://www.cert.org/archive/pdf/03tr001.pdf>

CERT-in-a-box

Perusteellinen kuvaus GOVCERT.NL:n ja Alankomaiden kansallisen varoituspalvelun (De Waarschuwingsdienst) perustamisen yhteydessä saaduista kokemuksista.

Lähde: <http://www.govcert.nl/render.html?it=69>

RFC 2350: Expectations for Computer Security Incident Response

Lähde: <http://www.ietf.org/rfc/rfc2350.txt>

NIST³⁷ Computer Security Incident Handling Guide

Lähde: <http://www.securityunit.com/publications/sp800-61.pdf>

ENISA Inventory of CERT activities in Europe

Hakuteos, jossa on tietoa eurooppalaisista CSIRT-ryhmistä ja niiden toiminnasta.

Lähde: http://www.enisa.europa.eu/cert_inventory/

³⁷ NIST: National Institute of Standards and Technologies.

A.2 CSIRT-palvelut

Kiitokset CERT/CC-ryhmälle, joka on laatinut tämän luettelon.

Reaktiiviset palvelut	Proaktiiviset palvelut	Artefaktien käsittely
Hälytykset ja varoitukset Tietoturvaloukkausten käsittely Tietoturvaloukkausten analysointi Tietoturvaloukkausten torjunta itse paikalla Tietoturvaloukkausten torjunnan tuki Tietoturvaloukkausten torjunnan koordinointi Heikkojen kohtien käsittely Heikkojen kohtien analysointi Haavoittuvuuden torjunta Haavoittuvuuden torjunnan koordinointi	Tiedotteet Teknologian seuranta Tietoturvatarkastukset tai -arvioinnit Tietoturvan määrittäminen ja ylläpitäminen Tietoturvatyökalujen kehittäminen Tunkeutumisen havaitseminen Tietoturvaan liittyvien tietojen jakaminen	Artefaktien analysointi Artefaktien torjunta Artefaktien torjunnan koordinointi
		<u>Tietoturvan laadun hallinta</u> Riskianalyysi Liiketoiminnan jatkuvuus ja vahingoista toipuminen Tietoturvaneuvonta Tietoisuuden lisääminen Koulutus/opetus Tuotteen arviointi tai sertifiointi

Kuva 19. CERT/CC-ryhmän laatima CSIRT-palveluja koskeva luettelo

Palvelujen kuvaukset

Reaktiiviset palvelut

Reaktiivisten palvelujen tarkoitus on vastata apua koskeviin pyyntöihin, CSIRT:n asiakaskunnan lähettämiin tietoturvaloukkauksia koskeviin raportteihin ja mahdollisiin CSIRT-järjestelmän uhkiin tai sitä vastaan tehtyihin hyökkäyksiin. Jotkin palvelut käynnistyvät kolmannen osapuolen tekemien ilmoitusten tai valvonta- tai IDS-lokien ja varoitusten perusteella.

Hälytykset ja varoitukset

Tähän palveluun sisältyy sellaisten tietojen jakaminen, joissa kuvataan tunkeutujan hyökkäystä, tietoturvan haavoittuvuutta, tunkeutumista koskevia varoituksia, tietokonevirusta tai virushuijausta. Palvelu kattaa myös suositukset lyhyen aikavälin toimintatavaksi ongelman ratkaisemiseksi. Kyseessä olevaan ongelmaan reagoidaan lähettämällä hälytys, varoitus tai tiedote, jossa asiakkaille kerrotaan toimista ja annetaan opastusta järjestelmien suojaamiseksi tai sellaisten järjestelmien palauttamiseksi, joita ongelma koskee. CSIRT-ryhmä voi tuottaa tietoa, tai palveluntarjoajat, muut CSIRT-ryhmät, tietoturva-asiantuntijat tai muut asiakkaat voivat levittää tietoa edelleen.

Tietoturvaloukkausten käsittely

Tietoturvaloukkausten käsittelyllä tarkoitetaan pyyntöjen ja raporttien vastaanottamista, luokittelua ja niihin vastaamista sekä tietoturvaloukkausten ja tapahtumien analysointia. Erityisiin torjuntatoimenpiteisiin voi sisältyä

- toimien toteuttaminen sellaisten järjestelmien ja verkkojen suojaamiseksi, joihin tunkeutujan toiminnalla on vaikutusta tai joita se uhkaa
- ratkaisujen ja torjuntastrategioiden tarjoaminen asiaan liittyvien tiedotteiden tai varoitusten pohjalta
- tunkeutujan toimien etsiminen verkon muista osista
- verkkoliikenteen suodattaminen
- järjestelmien uudelleenrakentaminen
- järjestelmien paikkaus tai korjaus
- muiden torjunta- tai korjausstrategioiden kehittäminen

Koska erityyppiset CSIRT-ryhmät käsittelevät tietoturvaloukkauksia eri tavoin, tällaiset palvelut luokitellaan lisäksi toteutettujen toimien ja annetun avun mukaan seuraavasti:

Tietoturvaloukkausten analysointi

Tietoturvaloukkausten analyseja on eritasoisia, ja niihin liittyy monia osapalveluja. Tietoturvaloukkausten käsittelyssä tutkitaan erityisesti tietoturvaloukkaukseen tai tapahtumaan liittyviä saatavilla olevia tietoja ja artefakteja ja niitä tukevia todisteita. Analyysin tarkoitus on tunnistaa tietoturvaloukkauksen laajuus, tietoturvaloukkauksen aiheuttamien vahinkojen laajuus, tietoturvaloukkauksen luonne ja käytettävissä olevat torjuntastrategiat tai korjaustoimenpiteet. CSIRT voi käyttää haavoittuvuus- ja artefaktianalyysin tuloksia (kuvattu jäljempänä) selvittääkseen tietyn järjestelmän tapahtumia ja laatiakseen tapahtumista perusteellisen ja ajantasainen analyysin. CSIRT vertaa toimenpiteitä ja tietoturvaloukkauksia keskenään määrittääkseen niiden väliset suhteet, suuntaukset, mallit tai tunkeutujien allekirjoitukset. Kaksi osapalvelua, jotka voidaan toteuttaa tehtävän, päämäärän ja CSIRT-ryhmän menettelyjen mukaan osana tietoturvaloukkausten analysointia ovat seuraavat:

Oikeudellisten todisteiden kerääminen

Todisteiden kerääminen tietoturvaloukkauksen kohteena olevasta tietojärjestelmästä sekä todisteiden säilytys, dokumentointi ja analysointi järjestelmään tehtyjen muutosten määrittämiseksi ja turvallisuutta vaarantavaan toimintaan johtavien tapahtumien rekonstruomiseksi. Tiedot ja todisteet on kerättävä siten, että saadaan aikaan aukoton ketju, jota voidaan käyttää tuomioistuimessa todisteita koskevien sääntöjen mukaisesti. Oikeudellisten todisteiden keräämiseen sisältyy mm. hyökkäyksen kohteena olevien järjestelmien kovalevyjen bittikuvioiden kopioiminen; järjestelmään mahdollisesti tehtyjen muutosten tarkistus, esim. uudet ohjelmat, tiedostot, palvelut ja käyttäjät; käynnissä olevien prosessien ja avointen porttien etsintä ja troijanhevosohjelmien ja -työkalujen etsintä. Näitä tehtäviä suorittavan CSIRT-henkilöstön on myös oltava valmis toimimaan asiantuntijatodistajina tuomioistuimessa.

Seuranta tai jäljitys

Tunkeutujan alkuperän jäljittäminen tai niiden järjestelmien yksilöiminen, joihin tunkeutuja on päässyt. Tässä toiminnossa selvitetään, miten tunkeutuja on päässyt hyökkäyksen kohteena oleviin järjestelmiin ja niihin liittyviin verkkoihin, mitä järjestelmiä pääsyn mahdollistamiseksi on käytetty, missä hyökkäyksen lähtöpiste on ollut ja mitä

muista järjestelmiä ja verkkoja hyökkäyksessä on käytetty. Toimintoon voi kuulua myös tunkeutujan identiteetin määrittäminen. Tämä työ voidaan tehdä yksin, mutta siihen liittyy usein yhteistyö lainvalvontaviranomaisten, Internet-palvelujentarjoajien tai muiden organisaatioiden kanssa.

Tietoturvaloukkausten torjunta itse paikalla

CSIRT-ryhmä antaa välitöntä apua tapahtumapaikalla ja auttaa asiakaskuntaa toipumaan tietoturvaloukkauksesta. CSIRT analysoi tietoturvaloukkauksen kohteena olevat järjestelmät ja suorittaa järjestelmien korjauksen ja palauttamisen sen sijaan, että se antaisi pelkästään tukea tietoturvaloukkauksen torjuntaan puhelimitse tai sähköpostitse (katso jäljempänä). Tämä palvelu kattaa kaikki paikallisella tasolla toteutettavat toimet, jotka ovat välttämättömiä, jos tietoturvaloukkausta epäillään tai jos se tapahtuu. Jos CSIRT-ryhmä sijaitsee muualla, ryhmän jäsenet matkustavat paikalle ja toteuttavat toimet. Muissa tapauksissa paikallinen ryhmä voi jo olla paikalla ja toteuttaa tietoturvaloukkausten torjuntaan liittyviä toimia osana ryhmän rutiiniväilyä. Näin on varsinkin silloin, kun tietoturvaloukkausten käsittely kuuluu järjestelmän tai verkon ylläpitäjän tai tietoturvakäyttäjien tavanomaisiin työtehtäviin (sen sijaan, että perustettu CSIRT-ryhmä hoitaisi ne).

Tietoturvaloukkausten torjunnan tuki

CSIRT avustaa ja opastaa hyökkäyksen kohteita toipumaan tietoturvaloukkauksista puhelimitse, sähköpostitse, faksitse tai asiakirjojen avulla. Tähän voi sisältyä teknistä apua kerätyn tiedon tulkinnaissa, yhteystietojen antamista tai torjunta- ja korjausstrategioihin liittyvää opastusta. Tähän ei sisälly tapahtumapaikalla toteutettavia tietoturvaloukkausten torjuntatoimia, kuten edellä on kuvattu. CSIRT-ryhmä antaa sen sijaan etäopastusta, jotta itse paikalla oleva henkilöstö voi itse suorittaa vahingoista toipumiseen tarvittavat työt.

Tietoturvaloukkausten torjunnan koordinointi

CSIRT koordinoi niiden osapuolten torjuntatoimia, joita tietoturvaloukkaus koskee. Näitä ovat yleensä hyökkäyksen kohde, muut hyökkäyksen vaikutuspiirissä olevat ja ne, jotka pyytävät apua hyökkäyksen analysoinnissa. Toimet voivat koskea myös osapuolia, jotka tarjoavat IT-tukea hyökkäyksen kohteelle, kuten Internet-palveluntarjoajia, muita CSIRT-ryhmiä ja tapahtumapaikalla olevia järjestelmän ja verkon ylläpitäjiä. Koordinointitoimiin voi kuulua yhteystietojen kerääminen, ilmoittaminen osapuolille niiden mahdollisesta osallisuudesta (hyökkäyksen kohteena tai lähteenä), tilastojen kerääminen osapuolten määrästä sekä tietojen vaihdon ja analysoinnin helpottaminen. Koordinointiin voi kuulua myös organisaation oikeudelliselle neuvonantajalle, henkilöstöosastolle ja PR-osastolle ilmoittaminen sekä yhteistyö niiden kanssa. Tähän sisältyy myös koordinointi lainvalvontaviranomaisten kanssa. Tähän palveluun ei sisälly tietoturvaloukkausten välitön torjunta paikalla.

Heikkojen kohtien käsittely

Heikkojen kohtien käsittelyyn sisältyy tietojen ja raporttien vastaanottaminen laitteistojen ja ohjelmistojen haavoittuvuudesta; heikkojen kohtien luonteen, mekanismien ja vaikutusten analysointi sekä käsittelystrategian luominen heikkojen kohtien havaitsemiseksi ja korjaamiseksi. Koska erityyppiset CSIRT-ryhmät käsittelevät

haavoittuvuutta eri tavoin, tällaiset palvelut luokitellaan toteutettujen toimien ja annetun avun mukaan seuraavasti:

Haavoittuvuuden analysointi

CSIRT-ryhmä suorittaa laitteistojen tai ohjelmistojen heikkojen kohtien teknistä analysointia ja tutkimusta. Tähän sisältyy epäilytjen heikkojen kohtien todentaminen ja laitteistojen ja ohjelmistojen tekninen tutkimus heikon kohdan sijainnin ja hyödyntämistavan määrittämiseksi. Analyysiin voi sisältyä lähdekoodien tarkistus käyttämällä virheiden tarkistusohjelmaa heikon kohdan sijainnin määrittämiseksi. Analyysissä voidaan myös yrittää toistaa ongelma testausjärjestelmässä.

Haavoittuvuuden torjunta

Tähän palveluun kuuluu sopivien toimenpiteiden määrittäminen haavoittuvuuden torjumiseksi tai korjaamiseksi. Siihen voi liittyä ohjelmakorjausten (patch), korjausten (fix) ja muiden korjaustoimien (workaround) kehittämistä ja tutkimusta. Tähän sisältyy myös torjuntastrategian ilmoittaminen toisille mahdollisesti laatimalla ja jakamalla tiedotteita tai varoituksia. Palveluun voi sisältyä torjunta asentamalla ohjelmakorjausohjelmistoja sekä suorittamalla korjauksia tai muita korjaustoimia.

Haavoittuvuuden torjunnan koordinointi

CSIRT-ryhmä ilmoittaa yrityksen eri osille tai asiakaskunnalle heikosta kohdasta ja jakaa tietoa siitä, miten se korjataan tai torjutaan. CSIRT vahvistaa, että haavoittuvuuden torjunnan strategia on toteutettu onnistuneesti. Tähän palveluun voi liittyä viestintä palveluntarjoajien, muiden CSIRT-ryhmien, teknisten asiantuntijoiden, asiakkaiden sekä niiden henkilöiden tai ryhmien kanssa, jotka ovat alun perin havainneet haavoittuvuuden tai ilmoittaneet siitä. Toteutettaviin toimiin kuuluvat myös haavoittuvuuden tai haavoittuvuusraportin analysoinnin helpottaminen; vastaavien asiakirjojen, ohjelmakorjausten ja muiden korjaustoimien julkaisusuunnitelmien koordinointi sekä eri osapuolten suorittamien teknisten analyysien yhdistäminen. Tähän palveluun voi liittyä julkisen tai yksityisen arkiston tai haavoittuvuustietoja koskevan tietokannan ylläpito ja vastaavien käsittelystrategioiden ylläpito.

Artefaktien käsittely

Artefaktilla tarkoitetaan järjestelmästä löydettyä tiedostoa tai kohdetta, jota voidaan käyttää järjestelmien tai verkkojen tarkasteluun tai hyökkäyksiin tai jota käytetään turvatoimien kiertämiseksi. Artefakteja ovat muun muassa tietokonevirukset, troijanhevosohjelmat, madot, exploit-koodit ja työkalut.

Artefaktien käsittelyyn liittyy sellaisia artefakteja koskevien tietojen ja artefaktien kopioiden vastaanottaminen, joita käytetään hyökkäyksissä, kohdetiedusteluissa ja muissa luvattomissa tai haitallisissa toimissa. Kun artefakti on vastaanotettu, sitä arvioidaan. Tähän kuuluu artefaktien luonteen, mekanismien, versioiden ja käytön analysointi sekä torjuntastrategioiden kehittäminen (tai ehdottaminen) näiden artefaktien havaitsemiseksi, poistamiseksi tai torjumiseksi. Koska erityyppiset CSIRT-ryhmät toteuttavat artefaktien käsittelytoimia eri tavoin, tällaiset palvelut luokitellaan edelleen toteutettujen toimien ja annetun avun mukaan:

Artefaktien analysointi

CSIRT-ryhmät suorittavat järjestelmässä havaitun artefaktin teknisen tutkimuksen ja analysoinnin. Tehtyyn analyysiin voidaan sisällyttää tiedostotyyppin ja artefaktin rakenteen tunnistaminen, uuden artefaktin vertaaminen aikaisempiin artefakteihin tai saman artefaktin muihin versioihin yhtäläisyyksien ja erojen havaitsemiseksi, sekä käänteistekniikka tai koodin purkaminen artefaktin tarkoituksen ja tehtävän määrittämiseksi.

Artefaktien torjunta

Tähän palveluun sisältyy tarkoituksenmukaisten toimien määrittäminen artefaktien havaitsemiseksi ja poistamiseksi järjestelmästä sekä toimet, joilla estetään artefaktien asennus. Tähän voi liittyä sellaisten allekirjoitusten luominen, jotka voidaan lisätä viruksentorjuntaohjelmiin tai IDS:ään.

Artefaktien torjunnan koordinointi

Tähän palveluun sisältyy artefaktia koskevien analyysien tulosten ja torjuntastrategioiden jakaminen ja yhdistäminen muiden tutkijoiden, CSIRT-ryhmien, palveluntarjoajien ja muiden turvallisuusasiantuntijoiden kanssa. Toimiin kuuluu ilmoittaminen muille ja teknisten analyysien yhdistäminen lukuisista eri lähteistä. Toimiin voi kuulua myös julkisen arkiston tai asiakasarkiston ylläpitäminen tunnetuista artefakteista, niiden vaikutuksista ja vastaavista torjuntastrategioista.

Proaktiiviset palvelut

Proaktiivisilla palveluilla pyritään parantamaan asiakaskunnan infrastruktuuria tai tietoturvamenettelyä, ennen kuin tietoturvaloukkaus tapahtuu tai se havaitaan. Ensisijaisena tavoitteena on torjua tietoturvaloukkaukset ja vähentää mahdollisten tietoturvaloukkausten vaikutusta ja laajuutta.

Tiedotteet

Tiedotteisiin kuuluvat muun muassa tunkeutumishälytykset, haavoittuvuusvaroitukset ja tietoturvatiedotteet. Tällaisissa tiedotteissa asiakkaille annetaan tietoa uusista kehityskuluista, joilla on vaikutuksia keskipitkällä tai pitkällä aikavälillä, kuten hiljattain havaitut heikot kohdat tai tunkeutumistyökalut. Tiedotteiden ansiosta asiakkaat voivat suojata järjestelmänsä ja verkkonsa hiljattain havaituilta ongelmilta, ennen kuin niitä voidaan käyttää hyväksi.

Teknologian kehityksen seuraaminen

CSIRT-ryhmä seuraa ja tarkkailee uusia teknisiä kehityskulkuja, tunkeutumistoimia ja niihin liittyviä suuntauksia tulevien uhkien havaitsemiseksi. Tarkasteltavat aiheet voidaan ulottaa kattamaan oikeudelliset ja lainsäädännölliset määräykset, yhteiskunnalliset tai poliittiset uhat ja kehittyvän teknologian. Tämä palvelu kattaa tietoturvaan liittyvien postituslistojen ja verkkosivujen seurannan sekä tieteseen, teknologiaan, politiikkaan ja valtionhallintoon liittyvien ajantasaisien uutisten ja artikkelien seuraamisen, jotta saadaan asiakasjärjestelmien ja -verkkojen tietoturvan kannalta merkityksellistä tietoa. Palveluun voi sisältyä myös viestintä kolmansien osapuolten eli alan viranomaisten kanssa, jotta varmistetaan, että saadut tiedot ja tehdyt tulkinnot ovat optimaalisia ja mahdollisimman tarkkoja. Tarjottavat palvelut voivat olla tiedotteita, suuntaviivoja tai suosituksia, jotka liittyvät etenkin keskipitkän ja pitkän aikavälin tietoturvakysymyksiin.

Tietoturvatarkastukset tai -arvioinnit

Tämä palvelu kattaa organisaation tietoturvainfrastruktuurin yksityiskohtaisen tarkastamisen ja analyysin organisaation standardien tai muiden sovellettavien toimialastandardien pohjalta. Siihen voi sisältyä myös organisaation tietoturvakäytäntöjen tarkastaminen. Tarjottavia tarkastus- tai arviointipalveluja on monenlaisia, kuten seuraavat:

Infrastruktuurin arviointi

Tässä yhteydessä tarkastetaan manuaalisesti laitteisto- ja ohjelmistokokoonpanot, reitittimet, palomuurit, palvelimet ja työasemat, jotta varmistetaan, että ne sopivat yhteen organisaation tai toimialan parhaiden tietoturvakäytäntöjen ja standardikokoonpanojen kanssa.

Parhaiden käytäntöjen arviointi

Työntekijöitä sekä järjestelmän ja verkon ylläpitäjiä haastatellaan sen määrittämiseksi, ovatko niiden tietoturvakäytännöt organisaatiossa määritetyn tietoturvapoliitikan tai tiettyjen toimialan standardien mukaisia.

Aineiston tarkistus skannaamalla

Aineisto tarkistetaan skannaamalla heikkojen kohtien tai virusten varalta sen määrittämiseksi, mitkä järjestelmät ja verkot ovat haavoittuvia.

Murtautumistestaus

Murtautumistestauksessa testataan kohteen turvallisuus hyökkäämällä tarkoituksellisesti sen järjestelmiin ja verkkoihin.

Tällaisten tarkastusten tai arviointien toteuttamiseen tarvitaan etukäteislupa ylemmältä johdolta. Organisaation politiikassa saatetaan kieltää jotkin tällaisista menetelmistä. Tällaiseen palveluun voi sisältyä sellaisten yhteisten menetelmien kehittäminen, joiden pohjalta testit tai arviot suoritetaan, sekä testauksesta, arvioinneista ja tarkastuksista vastaavan henkilöstön pätevyyttä tai sertifiointia koskevien vaatimusten laatiminen. Tämä palvelu voidaan myös ulkoistaa alihankkijalle tai tietoturvapalvelujen tarjoajalle, jolla on tarvittava asiantuntemus tarkastusten ja arviointien suorittamiseksi.

Tietoturvatyökalujen, sovellusten, infrastruktuurien ja palvelujen kokoonpano ja ylläpito

Tämän palvelun yhteydessä annetaan ohjeita siitä, miten CSIRT:n asiakaskunnan tai itse CSIRT-ryhmän käyttämien tietoturvatyökalujen, sovellusten ja yleisen tietokoneinfrastruktuurin kokoonpano ja ylläpito hoidetaan turvallisesti. Sen lisäksi, että CSIRT-ryhmä antaa ohjeita, se voi päivittää ja ylläpitää tietoturvatyökalujen ja palvelujen kokoonpanoa. Tällaisia ovat IDS, verkkoskannaus- tai seurantajärjestelmät, suodattimet, lisäosat (wrappers), palomuurit, virtuaaliset yksityisverkot (VPN) tai todentamismenetelmät. CSIRT-yksikkö voi tarjota tällaisia palveluja myös osana varsinaisia tehtäviään. CSIRT-ryhmä voi myös hoitaa palvelinten, työasemien, kannettavien tietokoneiden, taskutietokoneiden (PDA) ja muiden langattomien laitteiden kokoonpanon tai ylläpidon tietoturvaa koskevien suuntaviivojen mukaisesti. Tämä palvelu kattaa sellaisten työkalujen ja sovellusten kokoonpanoon tai käyttöön liittyvien ongelmien saattamisen johdon tietoon, jotka CSIRT:n mukaan altistavat järjestelmän mahdollisesti hyökkäykselle.

Tietoturvatyökalujen kehittäminen

Tämä palvelu kattaa sellaisten uusien asiakaskohtaisten välineiden kehittämisen, joita asiakaskunta tai CSIRT itse vaatii tai toivoo. Tällaisia palveluja voivat olla esimerkiksi ohjelmakorjausten (patch) laatiminen asiakaskunnan käyttämää räätälöityä ohjelmistoa varten tai vaarantuneiden isäntäkoneiden uudelleenrakentamiseen käytettävien ohjelmistojen suojattu jakelu. Palvelu voi kattaa myös sellaisten työkalujen tai komentosarjojen kehittämisen, joilla laajennetaan käytössä olevien tietoturvatyökalujen toiminnallisuutta. Tällaisia ovat esimerkiksi uusi ohjelmallisäke (plug-in) haavoittuvuus- tai verkkoskanneria varten, salaustekniikan käyttöä helpottavat komentosarjat tai automatisoidut korjaustiedostojen jakelumekanismit.

Tunkeutumisen havaitseminen

Tällaisia palveluja tarjoavat CSIRT-ryhmät tarkastavat IDS-lokitiedostot, analysoivat ja aloittavat toimia, joilla vastataan määritettyjen kynnyksarvojen mukaisiin tapahtumiin, tai välittävät eteenpäin varoituksia ennalta määritellyn palvelutasosopimuksen tai eskalointisuunnitelman mukaisesti. Tunkeutumisen havaitseminen ja siihen liittyvien turvallisuuslokioiden analysointi voi olla vaikea tehtävä – tämä koskee sekä sen määrittämistä, mihin sensorit sijoitetaan ympäristössä, että suurten tietomäärien kokoamista ja niiden analysoimista. Usein tietojen yhdistämiseksi ja tulkitsemiseksi tarvitaan erityisiä työkaluja tai asiantuntemusta, jotta pystytään tunnistamaan väärät hälytykset, hyökkäykset tai verkkotapahtumat ja toteuttamaan strategiat, joilla eliminoidaan tai minimoidaan tällaiset tapahtumat. Jotkin organisaatiot päättävät ulkoistaa nämä toiminnot kolmansille osapuolille, kuten tietoturvapalvelujen tarjoajille, joilla on enemmän kokemusta näiden palvelujen suorittamisesta.

Tietoturvaa koskevien tietojen jakaminen

Asiakaskunnalle tarjotaan kattavaa ja havainnollista tietokokoelmaa tietoturvan parantamisen helpottamiseksi. Tällaisia tietoja ovat muun muassa seuraavat:

- raportointia koskevat ohjeet ja CSIRT:n yhteystiedot
- hälytyksiä, varoituksia ja muita tiedotteita koskevat arkistot
- nykyisiä parhaita käytäntöjä koskeva dokumentaatio
- tietokoneiden tietoturvaa koskevat yleiset ohjeet
- toimintalinjat, menettelyt ja tarkistuslistat
- ohjelmakorjausten (patch) kehittäminen ja tiedonjakelu
- linkit palveluntarjoajien sivuille
- ajantasaiset tilastotiedot ja tietosuojaloukkausten raportoinnin suuntaukset
- muut tiedot, joilla voidaan parantaa yleisiä turvallisuuskäytäntöjä

CSIRT tai jokin toinen organisaatioelin (IT-osasto, henkilöstöosasto tai PR-osasto) voi kehittää näitä tietoja edelleen ja julkaista ne, ja näihin tietoihin voi sisältyä myös ulkoisista lähteistä, kuten muilta CSIRT-ryhmiltä, palveluntarjoajilta ja tietoturva-asiantuntijoilta saatua tietoa.

Tietoturvan laadunhallinta

Tämän luokan palvelut eivät kuulu yksinomaan tietoturvapalvelujen tai CSIRT-ryhmien tarjoamien palvelujen piiriin. Ne ovat yleisesti tunnettuja vakiintuneita palveluja, joilla pyritään parantamaan organisaation yleistä turvallisuutta. Edellä kuvattujen reaktiivisten ja proaktiivisten palvelujen tarjoamisesta saatujen kokemusten pohjalta CSIRT voi tuoda uusia näkökulmia tällaisiin laadunhallintapalveluihin, jollaisia ei ehkä muutoin olisi

saatavana. Näissä palveluissa otetaan huomioon palaute ja kokemukset, jotka on saatu käsiteltäessä tietoturvaloukkauksia, heikkoja kohtia ja hyökkäyksiä. Liittämällä tällaiset kokemukset vakiintuneisiin perinteisiin palveluihin (joita kuvataan jäljempänä) osana tietoturvan laadunhallintaprosessia voidaan parantaa organisaation pitkän aikavälin turvallisuustoimia. Organisaation rakenteesta ja vastuualueista riippuen CSIRT voi tarjota tällaisia palveluja tai osallistua niiden tarjoamiseen osana organisaation suurempaa yhteistyöryhmää.

Jäljempänä kuvataan, miten CSIRT:n asiantuntemuksesta voi olla hyötyä tällaisia tietoturvan laadunhallintapalveluja tarjottaessa.

Riskianalyysi

CSIRT-ryhmät voivat tuoda lisäarvoa riskianalyysihin ja -arviointeihin. Näin voidaan parantaa organisaation valmiuksia arvioida todellisia uhkia, antaa realistisia laadullisia ja määrällisiä arvioita tietovarantoihin kohdistuvista riskeistä sekä arvioida suojelun ja torjunnan strategioita. Tällaisia palveluja tarjoavat CSIRT-ryhmät tekisivät tietoturvaan liittyviä riskianalyyseja ja avustaisivat niissä uusien järjestelmien ja liiketoimien yhteydessä tai arvioisivat asiakkaan tietovarantoihin ja -järjestelmiin kohdistuvia uhkia ja hyökkäyksiä.

Liiketoiminnan jatkuvuus ja vahingoista toipumisen suunnittelu

Aiempien tapahtumien ja uusia tietoturvaloukkauksia tai -suuntauksia koskevien tulevaisuussennusteiden perusteella voidaan todeta, että yhä useammat tietoturvaloukkaukset voivat vahingoittaa vakavasti yrityksen liiketoimia. Siksi suunnittelussa olisi otettava huomioon CSIRT:n kokemukset ja suositukset sen osalta, miten tällaisiin tietoturvaloukkauksiin voidaan parhaiten vastata, jotta varmistetaan liiketoimien jatkuvuus. Tällaisia palveluja tuottavat CSIRT-ryhmät osallistuvat liiketoiminnan jatkuvuuden ja vahingoista toipumisen suunnitteluun tietokoneiden turvallisuuteen kohdistuvien uhkien ja hyökkäysten varalta.

Turvallisuusneuvonta

CSIRT-yksiköt voivat antaa neuvoja ja ohjeita parhaista asiakaskunnan liiketoimiin sovellettavista turvallisuuskäytännöistä. Tällaisia palveluja tarjoavat CSIRT-ryhmät osallistuvat uusien järjestelmien, verkkolaitteiden, ohjelmistosovellusten tai yrityksenlaajuisten liiketoimintamenettelyjen hankintaa, asentamista tai suojaamista koskevien suositusten ja vaatimusten laadintaan. Tämä palvelu kattaa ohjeiden ja tuen antamisen organisaation tai asiakaskunnan turvallisuuspolitiikkaa laadittaessa. Palveluun voi sisältyä myös todistuksen tai neuvojen antaminen lainsäädäntöelimille tai muille valtion elimille.

Tietoisuuden lisääminen

CSIRT-ryhmät voivat auttaa määrittämään, millä aloilla asiakkaat tarvitsevat lisätietoa ja ohjausta, jotta ne toimisivat entistä paremmin hyväksytyjen tietoturvakäytäntöjen ja organisaation tietoturvapoliittikan mukaisesti. Asiakaskunnan yleisen tietoisuuden parantaminen tietoturvasta paitsi lisää asiakkaiden tietämystä tietoturvaan liittyvistä kysymyksistä myös auttaa heitä toteuttamaan päivittäiset toimensa turvallisemmin. Näin voidaan vähentää onnistuneiden hyökkäysten määrää ja lisätä sen todennäköisyyttä, että asiakkaat havaitsevat hyökkäykset ja raportoivat niistä, jolloin palautumisaika vähenee ja menetykset voidaan minimoida tai välttää kokonaan.

Tällaisia palveluja tarjoavat CSIRT-ryhmät pyrkivät lisäämään tietoisuutta tietoturvasta laatimalla artikkeleita, julisteita, uutiskirjeitä, verkkosivustoja tai muita tietolähteitä, joiden avulla annetaan tietoa tietoturvan parhaista käytännöistä ja toteutettavista varotoimista. Tällaisiin toimiin voivat kuulua myös kokousten ja seminaarien suunnittelu, jotta asiakkaat pidetään ajan tasalla käynnissä olevista tietoturvamenettelyistä ja organisaation järjestelmään kohdistuvista mahdollisista uhista.

Koulutus

Tämä palvelu kattaa tiedon välittämisen asiakkaille tietokoneiden tietoturvaongelmista, ja siihen sisältyy seminaarien, työpajojen, kurssien ja luentojen järjestäminen. Tarkasteltavia aiheita voivat olla tietoturvaloukkausten raportointia koskevat ohjeet, tietoturvaloukkausten käsittelymenetelmät, käsittelyvälineet, torjuntamenetelmät ja muut tiedot, jotka ovat välttämättömiä tietoturvaloukkausten estämiseksi, havaitsemiseksi, raportoimiseksi ja käsittelemiseksi.

Tuotteiden arviointi ja sertifiointi

Tällaisten palvelujen yhteydessä CSIRT tekee arviointeja työkaluista, sovelluksista ja muista palveluista sen varmistamiseksi, että tuotteet ovat turvallisia ja CSIRT:n tai organisaation sisäisten tietoturvakäytäntöjen mukaisia. Arvioitavat työkalut ja sovellukset voivat olla avoimen lähdekoodin tuotteita tai kaupallisia tuotteita. Tällaista palvelua voidaan tarjota toteuttamalla arviointeja tai sertifiointiohjelmia sen mukaan, mitä standardeja organisaatio tai CSIRT käyttää.

A.3 Esimerkit

Kuvitteellinen CSIRT

Vaihe 0 - Mikä on CSIRT?

Malliesimerkiksi valitaan CSIRT-ryhmä, joka tarjoaa palveluja keskikokoiselle 200 työntekijän laitokselle. Laitoksella on oma tietotekniikkaosasto ja kaksi muuta sivutoimipistettä samassa maassa. Tietotekniikka on keskeisessä asemassa yhtiössä, sillä sitä käytetään sisäistä viestintää, tiedonsiirtoa ja vuorokauden ympäri tapahtuvaa (24x7) sähköistä liiketoimintaa varten. Laitoksella on oma verkko ja lisäyhteys Internetiin kahden eri Internet-palveluntarjoajan (ISP) välityksellä.

Vaihe 1: aloitusvaihe

Aloitusvaiheessa uusi CSIRT-ryhmä määritetään organisaation sisäiseksi tietoturvaryhmäksi, ja se tarjoaa palveluja toimeksiantajaorganisaatiolle, paikalliselle IT-osastolle ja henkilöstölle. Lisäksi sillä on avustava ja koordinoiva tehtävä yksittäisten toimistojen välillä tietoturvaloukkausten käsittelyssä.

Vaihe 2: Oikeiden palvelujen valinta

Alkuvaiheessa päätetään, että uusi CSIRT-ryhmä keskittyy pääasiassa muutamien keskeisten palvelujen tarjoamiseen työntekijöille.

Päätetään, että pilottivaiheen jälkeen voidaan pohtia palveluvalikoiman laajentamista ja että siihen voidaan lisätä "tietoturvan hallinnan palveluja". Tällaisen päätöksen tulee perustua pilottiasiakkailta saatuun palautteeseen, ja se tehdään tiiviissä yhteistyössä laadunvarmistusosaston kanssa.

Vaihe 3: Asiakaskunnan ja asianmukaisten viestintäkeinojen analysointi

Liikkeenjohdon ja asiakaskunnan avainhenkilöiden kanssa järjestetyssä ideariihessä tuotetaan riittävästi tietoa SWOT-analyysia varten. Sen perusteella voidaan päätellä, että seuraavat keskeiset palvelut ovat välttämättömiä:

- hälytykset ja varoitukset
- tietoturvaloukkausten käsittely (analyysi, tuen antaminen ja torjunnan koordinointi)
- tiedotteet

On varmistettava, että tiedottaminen on hyvin organisoitua, jotta saavutetaan mahdollisimman suuri osa asiakaskunnasta. Niinpä päätetään julkaista hälytykset, varoitukset ja tiedotteet tietoturvatiedotuksina erityisellä verkkosivulla ja jakaa ne käyttämällä postituslistaa. CSIRT käyttää tietoturvaloukkauksia koskevien raporttien vastaanottamiseen sähköpostia, puhelinta ja faksia. Seuraavassa vaiheessa on tarkoitus suunnitella yhtenäinen Internet-lomake.

Vaihe 4: Toimenkuvan määrittäminen

Kuvitteellisen CSIRT:n johdon on määriteltävä toimenkuva seuraavasti:

"Kuvitteellinen CSIRT antaa tietoa ja tukea toimeksiantajansa henkilöstölle vähentääkseen tietoturvaloukkauksiin liittyviä vaaroja ja ratkaistakseen tällaiset mahdolliset tapahtumat."

Kuvitteellinen CSIRT selventää näin, että se on yrityksen sisäinen tietoturvaryhmä ja että sen keskeisenä tehtävänä on käsitellä IT-alan tietoturvakysymyksiä.

Vaihe 5: Liiketoimintamallin määrittely

Rahoitusmalli

Koska yritys harjoittaa ympärivuorokautista (24x7) sähköistä liiketoimintaa ja sillä on ympäri vuorokauden toimiva IT-osasto, päätetään, että toimistoaikoina tarjotaan kattavaa palvelua ja toimistoaikojen ulkopuolella palveluja tarjotaan päivystysperiaatteella. Asiakaskunnalle tarjotaan palveluja maksutta, mutta mahdollisuutta tarjota palveluja myös ulkopuolisille asiakkaille tarkastellaan pilotti- ja arviointivaiheen aikana.

Tulomalli

Käynnistys- ja pilottivaiheen aikana CSIRT saa rahoitusta toimeksiantajayritykseltä. Pilotti- ja arviointivaiheen aikana keskustellaan lisärahoituksesta, johon liittyy myös mahdollisuus myydä palveluja ulkoisille asiakkaille.

Organisaatiomalli

Koska toimeksiantajaorganisaatio on pieni yritys, valitaan integroitu malli. Toimistoaikoina kolme työntekijää tarjoaa keskeisiä palveluja (tietoturvatiedotteiden jakelu ja tietoturvaloukkausten käsittely/koordinointi).

Yrityksen IT-osaston palveluksessa on jo asianmukaisesti pätevöitynyttä henkilöstöä. Kyseisen osaston kanssa sovitaan, että uusi CSIRT-ryhmä voi pyytää tarvittaessa väliaikaista tukea. Lisäksi voidaan turvautua päivystäviin toisen tason teknisiin asiantuntijoihin.

CSIRT-ydinryhmä muodostuu neljästä täyspäiväisesti työskentelevästä jäsenestä ja viidestä CSIRT-ryhmän lisäjäsenestä. Yksi näistä jäsenistä on myös käytettävissä vuorotyötä varten.

Henkilöstö

CSIRT-ryhmän johtajalla on kokemusta tietoturvasta sekä ensimmäisen ja toisen tason tuesta sekä kriisitilanteiden hallinnasta. Ryhmän muut kolme jäsentä ovat tietoturva-asiantuntijoita. IT-osaston CSIRT-ryhmän osa-aikaiset jäsenet ovat asiantuntijoita omalla vastuualueellaan yrityksen infrastruktuurissa.

Vaihe 6: Toimiston käyttö ja tietoturvapolitiikka

Toimiston laitteistot ja sijainti

Koska toimeksiantajayrityksellä on jo käytössä tehokas fyysinen turvajärjestelmä, uusi CSIRT-ryhmä on tältä osin hyvin turvattu. Hätätilanteissa tehtävää koordinoitua varten otetaan käyttöön niin kutsuttu "war room" -neuvottelutila. Salasaineistoa ja

arkaluonteisia asiakirjoja varten hankintaan tallelokero. Lisäksi otetaan käyttöön erillinen puhelinlinja ja vaihde, jotta helpotetaan ns. kuuman linjan palvelua toimistoaikoina, ja "päivystävä" matkapuhelin, johon vastataan toimistoajan ulkopuolella ja jonka puhelinnumero on sama.

Jo käytössä olevia laitteita ja yrityksen verkkosivuja voidaan hyödyntää, kun tiedotetaan CSIRT:hen liittyvistä kysymyksistä. Lisäksi otetaan käyttöön ja pidetään yllä postituslistaa, ja ryhmän jäsenten välistä sekä muiden ryhmien kanssa harjoitettavaa viestintää varten perustetaan rajoitettu foorumi. Kaikki henkilöstön jäsenten yhteystiedot tallennetaan tietokantaan, ja tulostettuja tietoja säilytetään tallelokerossa.

Sääntely

Koska CSIRT-ryhmä integroidaan osaksi yritystä, jolla on jo käytössä oma tietoturvapoliittikka, CSIRT-ryhmää koskevat toimintalinjat määrätään yrityksen oikeudellisen neuvonantajan kanssa.

Vaihe 7: Yhteistyömahdollisuuksien etsiminen

ENISAn hakemiston avulla voidaan nopeasti löytää samassa maassa sijaitsevia CSIRT-ryhmiä ja ottaa niihin yhteyttä. Eräs äskettäin rekrytoitu ryhmänjohtaja vieraili tällaisessa CSIRT-ryhmässä. Hän sai tietää kansallisen CSIRT-ryhmän toiminnasta ja osallistui ryhmän kokoukseen.

Tämä kokous oli erittäin hyödyllinen, sillä hän keräsi esimerkkejä työskentelymenetelmistä ja sai tukea muutamalta muulta ryhmältä.

Vaihe 8: Liiketoimintasuunnitelman edistäminen

Yrityksen historiasta päätettiin kerätä tietoja ja lukuja. Tästä on paljon hyötyä tietoturvatilannetta koskevalle tilastokatsaukselle. Tietojen ja lukujen keräämistä pitäisi jatkaa, kun CSIRT-ryhmä on perustettu ja toiminnassa, jotta tilastot pysyvät ajantasaisina.

Muihin kansallisiin CSIRT-ryhmiin otettiin yhteyttä, ja niitä haastateltiin liiketoimintasuunnitelmien osalta. Ne tarjosivat tukea keräämällä kalvoja, joissa oli tietoa tietoturvaloukkausten viimeaikaisesta kehityksestä ja tietoturvaloukkausten kustannuksista.

Tässä kuvitteellisessa CSIRT-ryhmän esimerkkitapauksessa ei ollut kiireellistä tarvetta vakuuttaa johtoa IT-toiminnan tärkeydestä, joten ei ollut vaikea saada suostumusta ensimmäiselle vaiheelle. Laadittiin liiketoimintasuunnitelma ja hankesuunnitelma sekä arvio perustamis- ja toimintakustannuksista.

Vaihe 9: Työnkulkujen ja toiminnallisten ja teknisten menettelyjen vahvistaminen

Kuvitteellinen CSIRT-ryhmä keskittyy keskeisten CSIRT-palvelujen tarjoamiseen:

- Hälytykset ja varoitukset
- Tiedotteet
- Tietoturvaloukkausten käsittely

Ryhmä kehitti hyvin toimivia menettelyjä, joita ryhmän jäsenten on helppo ymmärtää. Kuvitteellinen CSIRT-ryhmä rekrytoi myös oikeudellisen neuvonantajan, joka hoitaa vastuukysymyksiä ja tietoturvapoliittikkaa. Ryhmä kehitti hyödyllisiä työkaluja ja sai hyödyllistä tietoa toiminnallisista kysymyksistä keskustelemalla muiden CSIRT-ryhmien kanssa.

Tietoturvatiedoille ja tietoturvaloukkauksia koskeville raporteille laadittiin vakiomalli. Ryhmä käyttää RTIR:ää (Request Tracker for Incident Response) tietoturvaloukkausten käsittelemiseen.

Vaihe 10: Henkilöstön koulutus

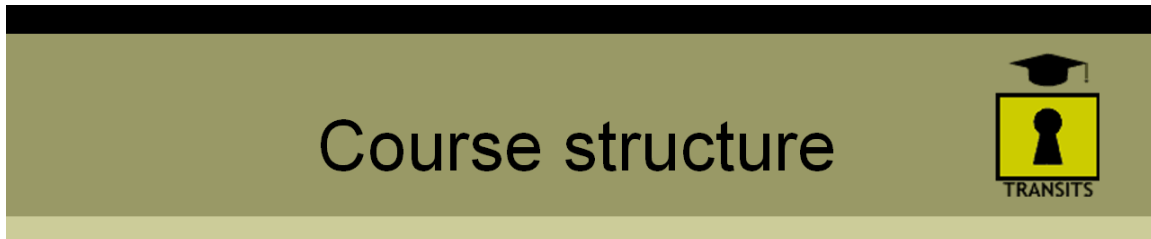
Kuvitteellinen CSIRT-ryhmä päätti lähettää teknisen henkilöstönsä seuraaville järjestettävälle TRANSITS-kursseille. Ryhmän johtaja osallistui myös CERT/CC-kurssille *CSIRT-ryhmän johtaminen*.

Vaihe 11: Harjoittelu

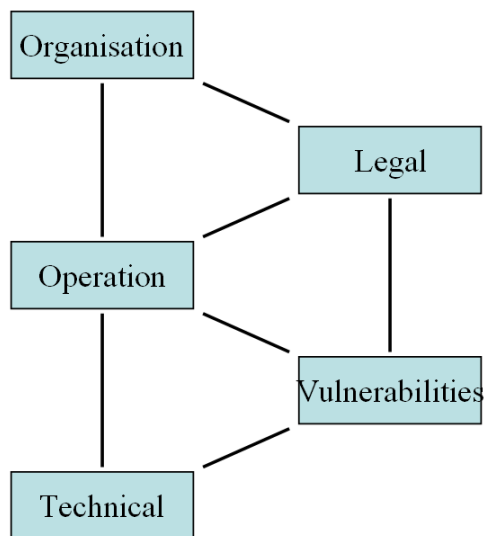
Toiminnan ensimmäisten viikkojen aikana kuvitteellinen CSIRT-ryhmä harjoitteli käyttämällä kuvitteellisia esimerkkitapauksia (jotka se sai muilta CSIRT-ryhmiltä). Lisäksi se antoi muutamia tietoturvatiedotuksia, jotka perustuivat laitteisto- ja ohjelmistotoimittajien jakamiin todellisiin heikkoja kohtia koskeviin tietoihin, joita ryhmä hienosäätö ja mukautti asiakaskunnan tarpeisiin.

A.4 Esimerkkiaineistoa CSIRT-kursseilta

TRANSITS-hanke (esitetään Terenan suostumuksella, <http://www.terena.nl>)



- Five modules
- Independent, but linked
- 12-14 hours work in 2 days
- Practical exercises include
 - Analyse incidents
 - Organisational plan
 - Incident response plan



CSIRT training course

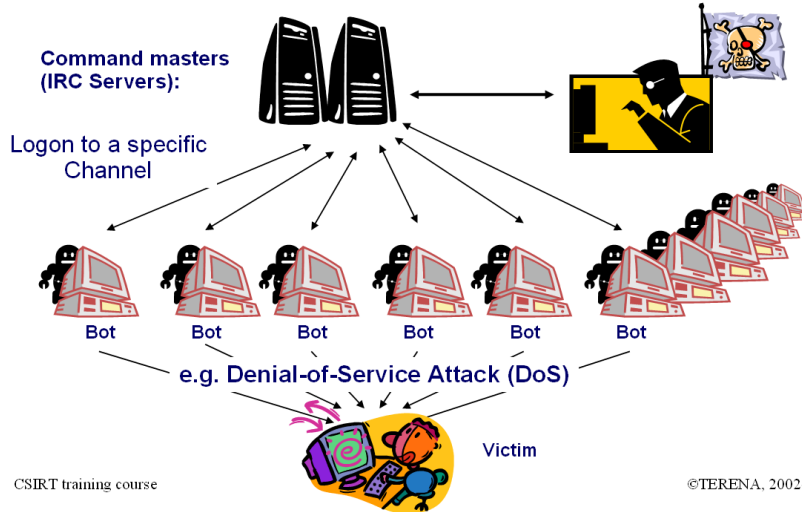
©TERENA, 2002-6



Yleiskuva: Kurssin rakenne

Malicious Code

Malicious IRC Bots - A botnet in action

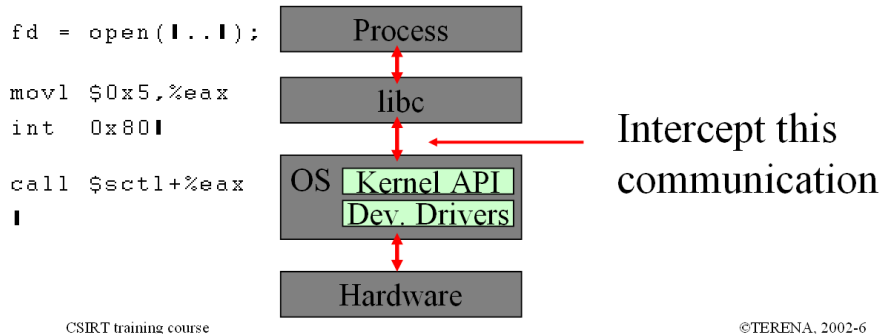
Tekninen moduuli: Botnet-verkon kuvaus

Malicious Code

Rootkits - Basic design



- Replacing binaries is easily detected (tripwire et al).
- A more elegant approach would deliver false data to **all** processes -> Modify kernel



Tekninen moduuli: Rootkit-ohjelmiston perusrakenne

Who is the Biggest Threat?

Employees?

- Secure h/w & s/w?
- Firewalls?
- Anti-virus s/w?



Viruses/Worms

LoveBug, CodeRed, Nimda, Slammer, ...

Cost \$1T worldwide

Need user help to spread:

- Unexpected attachments
- Unneeded programs

Unwary users get caught

Suppliers/Partners?

Do you know?

DTI* data indicates:

- 68% suffered a malicious incident
- Two thirds have no info security policy
- 57% have no contingency plan for incidents



Customers/Students?



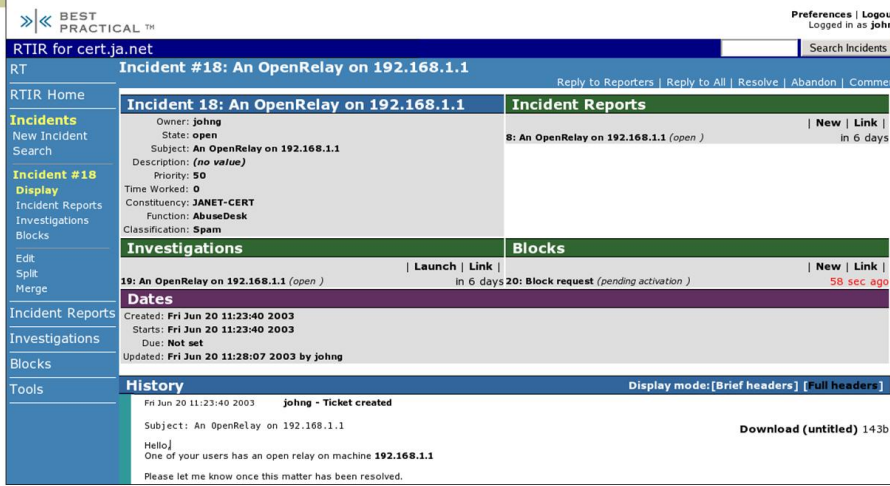
CSIRT training course

* UK Department for Trade & Industry Information Security Breaches survey 2004

©TERENA, 2002-6

Organisaatiomoduli: Sisäiset vai ulkoiset tahot – kumpi on suurempi uhka?

e.g. RTIR incident page



CSIRT training course

©TERENA, 2002-6

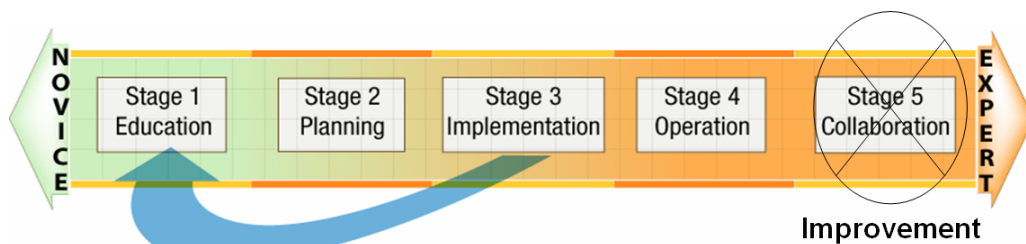
Tapahtumaseuranta: Request Tracker for Incident Response (RTIR)

"CSIRT-ryhmän perustaminen" (CERT/CC:n suostumuksella <http://www.cert.org>)

ENISA kiittää CERT-ohjelman CSIRT-kehittämisryhmää siitä, että se on antanut luvan käyttää koulutuskurssiensa sisältöä.

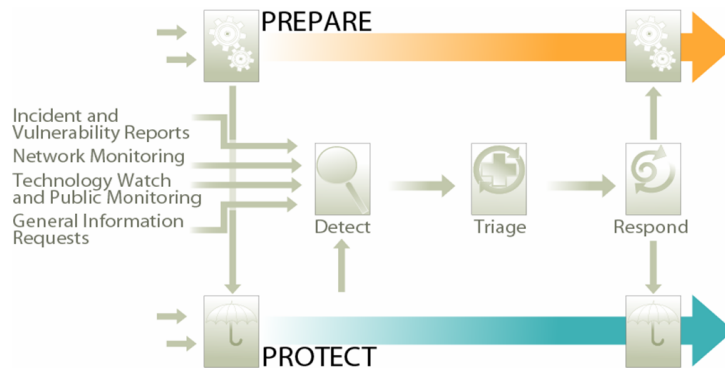
Stages of CSIRT Development

- Stage 1 Educating the organization
- Stage 2 Planning effort
- Stage 3 Initial implementation
- Stage 4 Operational phase
- Stage 5 ~~Peer collaboration~~ — Improvement of the CSIRT



CERT/CC:n koulutuskurssi: CSIRT-ryhmän kehittämisen vaiheet

Incident Management Best Practice Model



© 2006 Carnegie Mellon University

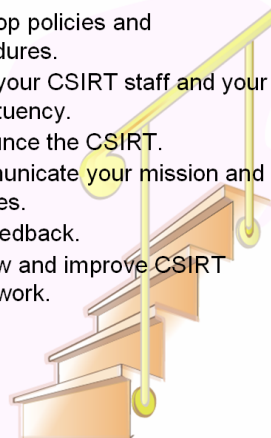
3



CERT/CC:n koulutuskurssi: Parhaat käytännöt tietoturvaloukkausten käsittelyssä

Basic Implementation Steps

- Gather information.
- Identify the CSIRT constituency.
- Determine the CSIRT mission.
- Secure funding for CSIRT operations.
- Determine CSIRT range and levels of service.
- Determine CSIRT reporting structure, authority and organizational model.
- Identify interactions with key parts of the constituency.
- Define roles and responsibilities for interactions.
- Create a plan, obtain feedback on the plan.
- Identify and procure personnel, equipment and infrastructure resources.
- Develop policies and procedures.
- Train your CSIRT staff and your constituency.
- Announce the CSIRT.
- Communicate your mission and services.
- Get feedback.
- Review and improve CSIRT framework.



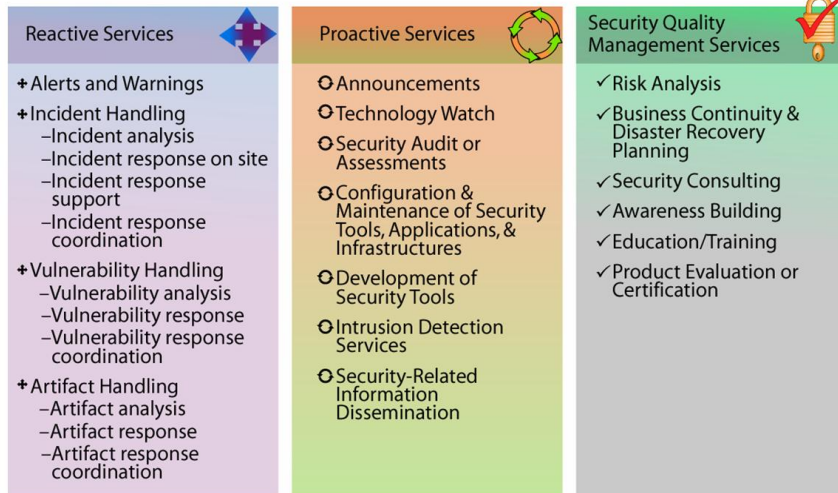
© 2006 Carnegie Mellon University

4



CERT/CC:n koulutuskurssi: CSIRT-ryhmän perustamisessa huomioon otettavat vaiheet

Range of CSIRT Services



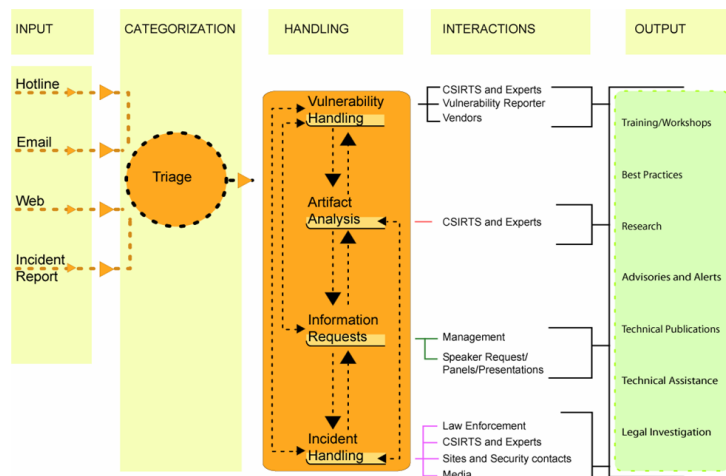
© 2006 Carnegie Mellon University

5



CERT/CC:n koulutuskurssi: CSIRT-ryhmän palveluvalikoima

Service Integration



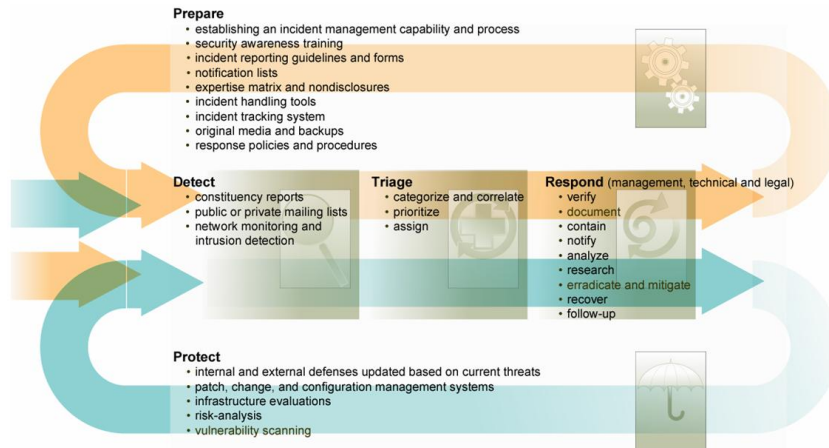
© 2006 Carnegie Mellon University

6



CERT/CC:n koulutuskurssi: Työnkulku tietoturvaloukkauksissa

Incident Response Starts Before an Incident Occurs



© 2006 Carnegie Mellon University

8

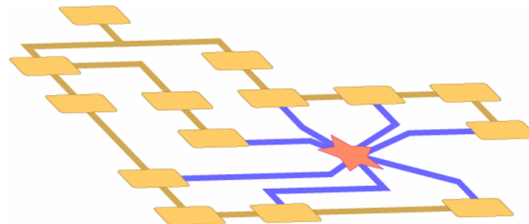


CERT/CC:n koulutuskurssi: Tietoturvaloukkauksiin reagoiminen

Organizational Models

When designing the vision of your CSIRT, you need to think about how the CSIRT will operate and interact with the organization and constituency.

You need to envision a model that can be implemented.



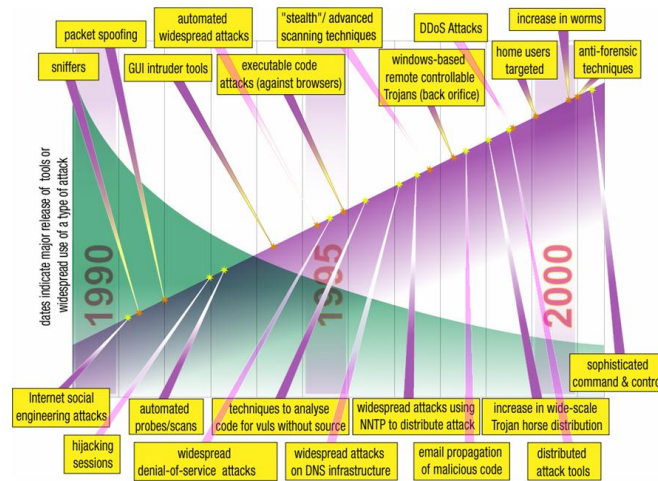
© 2006 Carnegie Mellon University

7



CERT/CC:n koulutuskurssi: CSIRT-ryhmän organisointi

Attack Sophistication versus Required Intruder Knowledge



© 2006 Carnegie Mellon University

9



CERT/CC:n koulutuskurssi: Mitä vähemmän tietoa, sen enemmän vahinkoja