SECĪGA CSIRT IZVEIDOŠANAS METODE

Uzdevums WP2006/5.1(CERT-D1/D2)

Saturs

1. Kopsavilkums

Šajā dokumentā aprakstīts Datoru drošības incidentu reaģēšanas vienības (CSIRT) izveides process, ņemot vērā visus attiecīgos aspektus, kā uzņēmējdarbības vadību, procesu pārvaldību un tehnisko aspektu. Dokuments īsteno divus no ENISA 2006. gada darbības programmas 5.1. nodaļā nospraustajiem uzdevumiem:

- šo dokumentu — ziņojumu, kas apraksta secīgu metodi CERT vai līdzīgas struktūras izveidošanai, minot piemērus (**CERT-D1**);
- 12. nodaļu un failus, kas neietilpst dokumentā — *detalizēts ceļveža izvilkums, kas nodrošina ceļveža ērtu pielietošanu praksē* (**CERT-D2**).

2. Juridisks paziņojums

3. Atzinības

ENISA vēlas pateikties visām iestādēm un personām, kas piedalījās šī dokumenta izstrādē. Īpaša pateicība pienākas:

- Henkam Bronkam (*Henk Bronk*), konsultantam, kas izstrādāja dokumenta sākotnējo versiju;
- CERT/CC un īpaši CSIRT attīstības vienībai, kas iesniedza ļoti noderīgus materiālus un kursa materiālu paraugu pielikumam;
- GovCERT.NL, kas sniedza *CERT-in-a-box* materiālu;
- TRANSITS komandai, kas iesniedza kursa materiālu paraugu pielikumam;
- kolēģiem no Tehniskā departamenta Drošības policijas nodaļas, kas palīdzēja izstrādāt 6.6. nodaļu;
- daudzajiem cilvēkiem, kas dokumentu pārskatīja.

4. Ievads

Komunikāciju tīkli un informācijas sistēmas kļuvušas par būtisku ekonomiskās un sociālās attīstības faktoru. Datoru ierīces un tīkli kļūst par ikdienas sastāvdaļu gluži tāpat kā elektrība un ūdens apgāde.

Tāpēc arvien vairāk pieaug sabiedrības bažas par komunikāciju tīklu un informācijas sistēmu drošību un īpaši to pieejamību. Bažas rada galveno informācijas sistēmu kļūmju risks, kas saistīts ar sistēmu sarežģītību, incidentiem, kļūdām un uzbrukumiem fiziskajai infrastruktūrai, kas nodrošina ES pilsoņu labklājībai būtiskus pakalpojumus.

Eiropas Tīklu un informācijas drošības aģentūra (ENISA)[1] tika nodibināta 2004. gada 10. martā. Tās nolūks ir nodrošināt kopienā augstu un efektīvu tīklu un informācijas drošības līmeni un izkopt tīklu un informācijas kultūru, kas kalpotu pilsoņu, patērētāju, uzņēmumu un sabiedriskā sektora organizāciju interesēm Eiropas Savienībā, tādējādi veicinot iekšējā tirgus raitu darbību.

Tādas Eiropas drošības kopienas kā CERT/CSIRT, datoru ļaunlietošanas apkarošanas vienības un WARPS sadarbojas jau vairākus gadus, lai veidotu drošāku internetu. ENISA plāno atbalstīt šo kopienu centienus, sniedzot informāciju par pasākumiem, lai nodrošinātu pienācīgu pakalpojumu kvalitātes līmeni. Turklāt ENISA plāno pilnveidot savu spēju sniegt konsultācijas ES dalībvalstīm un ES iestādēm jautājumos, kas attiecas uz specifiskām IT lietotāju grupām ar atbilstošiem drošības pakalpojumiem. Tāpēc, balstoties uz 2005. gadā izveidotās *ad hoc* darba grupas „CERT Sadarbība un atbalsts" secinājumiem, jaunā darba grupa risinās jautājumus, kas attiecas uz adekvātu drošības pakalpojumu sniegšanu („CERT pakalpojumi") konkrētiem lietotājiem (to kategorijām vai grupām).

ENISA atbalsta jaunu CSIRT izveidi, publicējot šo ziņojumu — „Secīga CSIRT izveidošanas metode, kas papildināta ar kontroljautājumiem", kas palīdzēs izveidot CSIRT.

[1] Eiropas Parlamenta un Padomes 2004. gada 10. marta Regula (EK) Nr. 460/2004, ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru. „Eiropas Kopienas aģentūra" ir ES izveidota iestāde, kuras mērķis ir īstenot konkrētus tehniskus, zinātniskus vai pārvaldības uzdevumus ES „Kopienas ietvaros" („pirmais balsts").

4.1. Mērķa auditorija

Ziņojuma primārā mērķa auditorija ir valsts un citas iestādes, kas izlēmušas izveidot CSIRT ar mērķi aizsargāt savu vai ieinteresēto pušu IT infrastruktūru.

4.2. Kā lietot šo dokumentu

Dokuments sniedz informāciju par to, kas ir datoru incidentu reaģēšanas vienība (CSIRT), kādus pakalpojumus tā var sniegt un kas jādara, lai to izveidotu. Lasītājam vajadzētu gūt labu un pragmatisku pārskatu par CSIRT izveides metodi, struktūru un saturu.

4. nodaļa. *„Ievads*"
Ziņojuma ievads

5. nodaļa. *„CSIRT plānošanas un izveides vispārīgā stratēģija"*
Pirmajā sadaļā aprakstīts, kas ir CSIRT. Tā arī sniedz informāciju par dažādām vidēm, kurās CSIRT var darboties un kādus pakalpojumus tā var sniegt.

6. nodaļa. *„Biznesa plāna sastādīšana"*
Šajā nodaļā aprakstīts, kāda biznesa pārvaldības pieeja izmantota izveides procesā.

7. nodaļa. *„Biznesa plāna virzīšana"*
Šajā nodaļā apskatīti jautājumi, kas saitīti ar darbības pamatojumu un finansēšanu

8. nodaļa. *"Operatīvo un tehnisko procedūru piemēri"*
Šajā nodaļā aprakstīta informācijas iegūšanas procedūra un tās apkopošana drošības biļetenā. Šajā nodaļā aprakstīta arī darbplūsma, strādājot ar incidentiem.

9. nodaļa. *„CSIRT apmācība"*
Šajā nodaļā sniegts kopsavilkums par pieejamo CSIRT apmācību. Kursa materiālu paraugs ir sniegts kā piemērs pielikumā.

10. nodaļa. *„Vingrinājums*: *konsultatīva materiāla izveide"*
Šajā nodaļā ir vingrinājums par to, kā sniegt vienu no CSIRT pamatpakalpojumiem — sastādīt drošības biļetenu (jeb konsultatīvo materiālu).

12. nodaļa. „Projekta plāna apraksts"
Šajā nodaļa apskatīts papildinātais projekta plāns (kontroljautājumi), kas sniegts kopā ar šo rokasgrāmatu. Plāna nolūks ir sniegt ērti lietojamu rīku rokasgrāmatas ieviešanai.

4.3. Dokumentā lietotais formāts

Lai lasītājam sniegtu norādes, katra nodaļa sākas ar CSIRT izveides procesā līdz šim veikto pasākumu kopsavilkumu. Kopsavilkumi ir apvilkti ar šādu rāmi:

Pirmais uzdevums ir izpildīts.

Katras nodaļas nobeigumā ir praktisks apspriesto uzdevumu piemērs. Šajā dokumentā „Fiktīvā CSIRT" ir neliela, neatkarīga CSIRT vienība vidēja lieluma uzņēmumā vai iestādē. Kopsavilkums ir atrodams pielikumā.

Fiktīvā CSIRT

5. CSIRT plānošanas un izveides vispārīgā stratēģija

Lai sekmīgi sāktu CSIRT izveides procesu, jābūt skaidram redzējumam par iespējamiem pakalpojumiem, ko vienība sniegs saviem klientiem, ko „CSIRT pasaulē" parasti sauc par „klientūras pārstāvjiem". Tāpēc, lai laicīgi un kvalitatīvi sniegtu piemērotus pakalpojumus, jāizprot, kādas ir klientūras pārstāvju vajadzības.

5.1. Kas ir CSIRT?

CSIRT nozīmē *Computer Security Incident Response Team* — datoru drošības incidentu reaģēšanas vienība. Terminu „CSIRT" pamatā lieto Eiropā autortiesību aizsargātā „CERT" termina vietā, ko ASV ir reģistrējis CERT koordinācijas centrs (CERT/CC).
Šo vienību apzīmēšanai pastāv dažādi saīsinājumi:

- CERT vai CERT/CC (*Computer Emergency Response Team / Coordination Center*) - datoru avāriju reaģēšanas vienība/koordinācijas centrs)
- CSIRT (*Computer Security Incident Response Team* — datoru drošības incidentu reaģēšanas vienība)
- IRT (*Incident Response Team* — incidentu reaģēšanas vienība)
- CIRT (*Computer Incident Response Team* — datoru incidentu reaģēšanas vienība)
- SERT (*Security Emergency Response Team* — ārkārtas drošības situāciju reaģēšanas vienība)

Pirmais lielākais vīrusa uzliesmojums globālajā IT infrastruktūrā notika pagājušā gadsimta 80. gadu beigās. Vīrusu nosauca par *Morris*[2], tas strauji izplatījās, faktiski inficējot daudzas IT sistēmas visā pasaulē.

Šis atgadījums iedarbojās kā modinātājzvans — cilvēki pēkšņi atskārta, ka, lai tiktu galā ar līdzīgiem gadījumiem, ir ļoti nepieciešama sadarbība un koordinācija starp sistēmu administratoriem un IT vadītājiem. Tā kā laikam bija kritiska nozīme, vajadzēja izveidot labāk organizētu un strukturētu pieeju IT drošības incidentu risināšanai. Un tā dažas dienas pēc *Morris* incidenta *DARPA* (*Defence Advanced Research Projects Agency* — Padziļināto aizsardzības izpētes projektu aģentūra) izveidoja pirmo CSIRT: CERT koordinācijas centru (*CERT/CC*[3]), kas atradās Karnegi Mellona Universitāte Pitsburgā (Pensilvānija).

Šo modeli drīz vien pārņēma Eiropā, un 1992. gadā Holandes akadēmisko pakalpojumu sniedzējs *SURFnet* atklāja pirmo CSIRT Eiropā — *SURFnet-CERT*[4]. Pēc tam tikai izveidotas daudzas vienības, un pašlaik ENISA „Uzskaitē par CERT aktivitātēm Eiropā"[5] ir ziņas par 100 vienībām, kas atrodas Eiropā.

Gadu gaitā CERT vienības pilnveidoja savu rīcībspēju un no vienkāršas reaģēšanas grupām pārtapa par pilnvērtīgiem drošības pakalpojumu sniedzējiem, piedāvājot tādus

[2] Plašāka informācija par *Morris* vīrusu 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/

preventīvos pakalpojumus kā brīdināšanas, konsultatīvo drošības materiālu, apmācības un drošības pārvaldības pakalpojumus. Drīz vien radās viedoklis, ka termins „CERT" nav pietiekams. Rezultātā 19. gs. 90. gadu beigās tika radīts jauns termins „CSIRT". Pašreiz abus terminus (CERT un CSIRT) lieto kā sinonīmus, bet CSIRT ir precīzāks.

5.1.1. Termins „klientūra"

Tālāk tekstā ar CSIRT kopienās labi pazīstamo terminu „klientūra" apzīmēs CSIRT klientu bāzi. Vienu klientu sauks par „klientūras pārstāvi" un to grupu par „klientūras pārstāvjiem".

5.1.2. CSIRT definīcija

CSIRT vienība ir IT drošības ekspertu grupa, kuras pamatnodarbošanās ir reaģēt uz datoru drošības incidentiem. Tā sniedz pakalpojumus, kas nepieciešami, lai risinātu incidentus un atbalstītu klientūru, palīdzot klientiem likvidēt ielaušanās sekas.

Lai mazinātu risku un tiešās iejaukšanās gadījumu skaitu, vairums CSIRT savai klientūrai sniedz arī preventīvos un izglītības pakalpojumus. Tās izdod konsultatīvus materiālus par izmantoto programmatūru un aparatūru ievainojamībām, kā arī informē lietotājus par ielaušanās mēģinājumiem un vīrusiem, kas cenšas šos trūkumus izmantot. Tādējādi klientūras pārstāvji var ātri pielabot un atjaunināt savas sistēmas. Pilnu sarakstu ar iespējamiem pakalpojumiem skatīt 5.2. nodaļā „Iespējamie pakalpojumi".

5.1.3. CSIRT sniegtās priekšrocības

Specializētas IT drošības vienības pakalpojumi palīdz organizācijai samazināt un novērst būtiskus incidentus un palīdz aizsargāt vērtīgu īpašumu.

Papildu priekšrocības ir:

- centralizēta IT drošības jautājumu koordinācija organizācijas ietvaros (kontaktpunkts),
- centralizēta un specializēta rīcība un reakcija IT incidentu gadījumā,
- ērti pieejama speciālā palīdzība, lai lietotāji varētu ātri likvidēt drošības incidentu sekas,
- juridisku jautājumu kārtošana un pierādījumu saglabāšana tiesas procesa gadījumā,
- informācija par jaunumiem drošības jomā,
- sadarbības veicināšana klientūras vidū par IT drošības jautājumiem (izpratnes veidošana).

Fiktīvā CSIRT (0. uzdevums)
Gūt izpratni par to, kas ir CSIRT Piemērā minētā CSIRT apkalpo vidēja lieluma iestādi, kurā strādā 200 darbinieki. Šai iestādei ir sava IT nodaļa un divas filiāles, kas atrodas tai pašā valstī. Šajā uzņēmumā IT ir būtiska nozīme, jo to izmanto iekšējai saziņai, datu tīklam un 24x7 e-darījumiem. Iestādei ir savs tīkls un rezerves pieslēgums internetam, un tā saņem pakalpojumus no diviem atšķirīgiem interneta pakalpojumu sniedzējiem.

5.1.4. CSIRT darbības vides veidu apraksts

Pirmais uzdevums ir izpildīts.

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.

>> Nākamais uzdevums ir atbildēt uz jautājumu: „Kādam sektoram tiks sniegti CSIRT pakalpojumi?"

Veidojot CSIRT (tāpat kā veidojot jebkuru citu uzņēmumu), jau pašā sākumā ir svarīgi rast skaidru priekšstatu par to, kas būs ieinteresēta klientūra un kādai videi CSIRT pakalpojumi tiks veidoti. Pašlaik izšķir šādus darbības „sektorus":

- akadēmiskā sektora CSIRT
- komerciālā sektora CSIRT
- CIP/CIIP (kritiskās informācijas un kritiskās informācijas infrastruktūras aizsardzības) sektora CSIRT
- valsts pārvaldes sektora CSIRT
- organizācijas iekšējā CSIRT
- militārā sektora CSIRT
- valsts CSIRT
- mazo un vidējo uzņēmumu (MVU) sektora CSIRT
- tirdzniecības sektora CSIRT

Akadēmiskā sektora CSIRT
Galvenais interešu loks
Akadēmiskā sektora CSIRT sniedz CSIRT pakalpojumus tādām akadēmiskām un izglītības iestādēm kā universitātēm, pētniecības institūtiem un to pilsētiņās izmantotai interneta videi.

Ieinteresētā klientūra
Tipiska šāda veida CSIRT klientūra ir universitāšu darbinieki un studenti.

Komerciālā sektora CSIRT
Galvenais interešu loks
Komerciālā CSIRT sniedz savai klientūrai CSIRT pakalpojumus uz komerciāliem pamatiem. Interneta pakalpojumu sniedzēja gadījumā CSIRT gala lietotājiem galvenokārt sniedz pakalpojumus, novēršot ļaunlietošanu (iezvanīšana, ADSL), un CSIRT pakalpojumus profesionāliem klientiem.

Ieinteresētā klientūra
Komerciālās CSIRT vienības parasti sniedz pakalpojumus klientūrai, kas par to maksā.

CIP/CIIP sektora CSIRT
Galvenais interešu loks
Šī sektora CSIRT vienības galvenokārt pievērš uzmanību svarīgas informācijas aizsardzībai un/vai svarīgas informācijas un infrastruktūras aizsardzībai. Vairumā gadījumu tā ir specializēta CSIRT, kas strādā ciešā sadarbībā ar valsts svarīgas informācijas un infrastruktūras aizsardzības departamentu. Tā aptver visus kritiski svarīgos IT sektorus valstī un aizsargā attiecīgās valsts pilsoņus.

Ieinteresētā klientūra
Valdība, svarīgie IT uzņēmumi, pilsoņi.

Valsts pārvaldes sektora CSIRT
Galvenais interešu loks
Valsts pārvaldes CSIRT sniedz pakalpojumus valdības aģentūrām un dažās valstīs arī pilsoņiem.

Ieinteresētā klientūra
Valdība un ar valsts pārvaldi saistītas aģentūras; dažās valstīs brīdināšanas pakalpojumi tiek sniegti arī pilsoņiem (piemēram, Beļģijā, Ungārijā, Nīderlandē, Apvienotajā Karalistē un Vācijā).

Organizācijas iekšējā CSIRT
Galvenais interešu loks
Iekšējā CSIRT sniedz pakalpojumus tikai savas mītnes organizācijai. Tas drīzāk raksturo funkciju, nevis sektoru. Piemēram, daudzām telekomunikāciju organizācijām un bankām ir savas iekšējās CSIRT vienības. Parasti tās neuztur tīmekļa vietni publiskai lietošanai.

Ieinteresētā klientūra
Mītnes organizācijas darbinieki un IT nodaļa.

Militārā sektora CSIRT
Galvenais interešu loks
Šajā sektorā CSIRT sniedz pakalpojumus militārām organizācijām, kas atbild par aizsardzības vajadzībām paredzētu IT infrastruktūru.

Ieinteresētā klientūra
Militāro iestāžu personāls vai ar to cieši saistītās vienības, piemēram, Aizsardzības departaments.

Valsts CSIRT
Galvenais interešu loks
CSIRT, kas veic darbību valstī un kas kalpo kā kontaktpunkts drošības jautājumos konkrētajā valstī. Dažos gadījumos valsts pārvaldes CSIRT darbojas arī kā valsts mēroga kontaktpunkts (kā piemēram, UNIRAS Apvienotajā Karalistē).

Ieinteresētā klientūra
Šī veida CSIRT vienībai parasti nav tiešas klientūras, jo valsts CSIRT vienībai ir tikai starpnieka loma valsts mēroga vajadzību apmierināšanai.

Mazo un vidējo uzņēmumu (MVU) sektora CSIRT
Galvenais interešu loks
Uzņēmumu organizēta CSIRT, kas sniedz pakalpojumus savai nozarei vai līdzīgai lietotāju grupai.

Ieinteresētā klientūra
Šo CSIRT vienību ieinteresētā klientūra varētu būt MVU un to darbinieki vai īpašas interešu grupas, piemēram, valsts „Pilsētu un vietējo pašvaldību asociācija"

Tirdzniecības sektora CSIRT
Galvenais interešu loks
Tirdzniecības CSIRT galvenokārt pievērš uzmanību konkrēto tirgotāju produktu atbalstam. Parasti tās nolūks ir izstrādāt un sniegt risinājumus, lai novērstu ievainojamības un samazinātu potenciālās nepilnību radītās sekas.

Ieinteresētā klientūra
Produktu īpašnieki.

Kā aprakstīts sadaļā par valsts CSIRT, viena vienība var apkalpot vairāk nekā vienu sektoru. Tas, piemēram, ietekmē klientūras un tās vajadzību analīzi.

Fiktīvā CSIRT (1. uzdevums)
Sākuma posms Sākuma posmā jaunā CSIRT tiek plānota kā iekšēja CSIRT, kas sniedz pakalpojumus mītnes uzņēmumam, vietējai IT nodaļai un darbiniekiem. Tā arī atbalsta un koordinē rīcību starp dažādām filiālēm IT drošības incidentu gadījumā.

5.2. Iespējamie pakalpojumi, ko CSIRT var sniegt

Pirmie divi uzdevumi ir izpildīti.

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.
2. Kādam sektoram tiks sniegti jaunās CSIRT vienības pakalpojumi?

>> Nākamais uzdevums ir atbildēt uz jautājumu: „Kādus pakalpojumus sniegt klientūras pārstāvjiem?"

CSIRT var sniegt daudzus pakalpojumus, bet līdz šim neviena CSIRT vienība nav mēģinājusi sniegt visus iespējamos. Piemērotas pakalpojumu kopas izvēle ir izšķirīgs lēmums. Tālāk tekstā dots īss pārskats par visiem zināmajiem CSIRT pakalpojumiem, kas definēti „CSIRT rokasgrāmatā", ko publicējis CERT/CC[6].

[6] *CERT/CC* CSIRT rokasgrāmata: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Reaģēšanas pakalpojumi	**Proaktīvas rīcības pakalpojumi**	**Darinājumu apstrāde**
• **trauksmes un brīdinājumi** • **darbs ar incidentiem** • **incidentu analīze** • **atbalsts, reaģējot uz incidentiem** • **koordinācija, reaģējot uz incidentiem** • reaģēšana uz incidentiem uz vietas • darbs ar ievainojamību • ievainojamības analīze • reaģēšana uz ievainojamību • koordinācija, reaģējot uz ievainojamību	• **paziņojumi** • tehnoloģijas uzraudzīšana • drošības auditi vai novērtējumi • drošības konfigurēšana un uzturēšana • drošības rīku izveide • ielaušanās atklāšanas pakalpojumi • ar drošību saistītas informācijas izplatīšana	• *darinājumu analīze* • *reaģēšana uz darinājumiem* • *koordinēšana, reaģējot uz darinājumiem* ***Drošības kvalitātes vadība*** • *riska analīze* • *darbības nepārtrauktība un seku likvidācija* • *konsultācijas drošības jautājumos* • *izpratnes veidošana* • *izglītība, apmācība* • *produktu vērtēšana vai sertifikācija*

1. att. CSIRT pakalpojumu saraksts no CERT/CC[7]

Pamatpakalpojumi (atzīmēti treknā drukā) — izšķir reaģēšanas un proaktīvas rīcības pakalpojumus. Proaktīvu pakalpojumu mērķis ir novērst incidentus, veidojot izpratni un rīkojot apmācības, bet reaģēšanas pakalpojumu mērķis ir strādāt ar incidentiem un mazināt to radītos bojājumus.

Darbs ar darinājumiem ietver to failu vai objektu analīzi, kas konstatēti sistēmā un kas varētu būt saistīti ar ļaunprātīgām darbībām, kā vīrusu paliekas, tārpi, skripti, Trojas zirgi u.c. Tas ietver iegūtas informācijas apstrādi un izplatīšanu tirgotājiem un citām ieinteresētājam personām, lai novērstu tālāku ļaundabīgās programmatūras izplatīšanos vai mazinātu risku.

Drošības un kvalitātes vadības pakalpojumi ir pakalpojumi ar ilgtermiņa mērķiem, un tie ietver konsultācijas un izglītības pasākumus.

Sīkāku paskaidrojumu par CSIRT pakalpojumiem skatīt pielikumā.

Ieinteresētajai klientūrai piemērotu pakalpojumu izvēle ir svarīgs uzdevums, un tas tiks vēl apskatīts 6.1. nodaļā „Finanšu modeļa definēšana”.

Vairums CSIRT sāk savu darbību, izplatot klientūrai trauksmes un brīdinājuma ziņojumus, sniedzot paziņojumus un strādājot ar incidentiem. Šie pamatpakalpojumi parasti nodrošina labu publicitāti, piesaista klientūras uzmanību, un būtībā uzskatāmi par patieso „papildvērtību".

[7] CSIRT pakalpojumu saraksts no *CERT/CC*: http://www.cert.org/csirts/services.html

Labā prakse ir sākt darbu ar nelielu izmēģinājuma klientūras grupu, izmēģinājuma periodā sniegt tiem pamatpakalpojumus un pēc tam lūgt tos komentēt.
Ieinteresētie izmēģinājuma perioda lietotāji parasti sniedz konstruktīvas atsauksmes un palīdz izveidot klientu vajadzībām pielāgotus pakalpojumus.

Fiktīvā CSIRT (2. uzdevums)
Piemērotu pakalpojumu izvēle Sākuma posmā tiek nolemts, ka jaunās CSIRT vienības darbība koncentrēsies galvenokārt uz pamatpakalpojumu sniegšanu darbiniekiem. Tiek nolemts, ka pakalpojumu klāsta paplašināšana tiks apsvērta pēc izmēģinājuma posma un, iespējams, tiks piedāvāti arī drošības vadības pakalpojumi. Lēmumu pieņems, balstoties uz komentāriem, ko sniegs izmēģinājuma posma klientūra, un ciešā sadarbībā ar kvalitātes nodrošināšanas nodaļu.

5.3. Klientūras analīze un misijas formulējums

Pirmie trīs uzdevumi ir izpildīti.

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.
2. Kādam sektoram tiks sniegti jaunās CSIRT vienības pakalpojumi?
3. Kāda veida pakalpojumus CSIRT var sniegt savai klientūrai.

>> Nākamais uzdevums ir atbildēt uz jautājumu: „Kādu metodi izvēlēties CSIRT darbības uzsākšanai?"

Šā uzdevuma mērķis ir dziļāk analizēt klientūru, lai noskaidrotu piemērotākos saziņas kanālus:

- pieejas definēšana saziņai ar klientūru,
- misijas formulēšana,
- reālistiska ieviešanas vai projekta plāna sastādīšana,
- CSIRT pakalpojumu noteikšana,
- organizācijas struktūras noteikšana,
- informācijas drošības politikas formulēšana,
- atbilstoša personāla algošana,
- CSIRT biroja izmantošana,
- CSIRT un iespējamo valsts iniciatīvu sadarbības iespēju noskaidrošana.

Šie uzdevumi ir detalizētāk aprakstīti tālāk tekstā, un tie var būt noderīgi biznesa un projekta plāna izveidē.

5.3.1. Pieeja saziņai ar klientūru

Ka minēts iepriekš, ļoti svarīgi ir izzināt klientūras vajadzības un izvēlēties saziņas stratēģiju, ieskaitot saziņas kanālus, kas ir visvairāk piemēroti klientu informēšanai.

Vadības teorijā ir zināmas vairākas pieejas mērķa grupas analizēšanai. Šajā dokumentā aprakstītas divas no tām: SVID (SWOT) un PEST analīze.

SVID (SWOT) analīze
SVID analīze ir stratēģiskās plānošanas rīks, ko izmanto lai izvērtētu kāda projekta vai komerciāla pasākuma, vai jebkādas citas situācijas — kurā jāpieņem lēmums — **s**tipros un **v**ājos punktus, **i**espējas un **d**raudus. Par šīs metodes autoru tiek uzskatīts Alberts Humfrejs *(Albert Humphrey*), kas 19. gs. 60. un 70. gados Stenfordas Universitātē vadīja izpētes projektu, izmantojot datus no Fortune 500.[8]

stiprā puse	**vājā puse**
iespējas	**draudi**

2. att. SVID (SWOT) analīze

[8] SVID (SWOT) analīze Vikipēdijā: http://en.wikipedia.org/wiki/SWOT_analysis

PEST analīze

PEST analīze ir vēl viena svarīga un plaši izmantota klientūras analīzes metode, kuras mērķis ir noskaidrot **p**olitiskos, **e**konomiskos, **s**ociālos un **t**ehnoloģiskos faktorus vidē, kurā darbojas CSIRT. Tā palīdz noskaidrot, vai plānošana joprojām atbilst konkrētajai videi, un var palīdzēt izvairīties no darbībām, kas veiktas, balstoties uz nepareiziem pieņēmumiem.

Politiskie faktori	**Ekonomiskie faktori**
• ekoloģiskie jeb vides jautājumi • pašreizējā likumdošana vietējā tirgū • nākotnes likumdošana • Eiropas vai starptautiskā likumdošana • regulatīvās iestādes un procesi • valdības politika • valdības darbības periods un maiņa • tirdzniecības politika • finansējums, granti un iniciatīvas • lobēšanas grupas vietējā tirgū • starptautiskās sabiedriskās domas ietekmēšanas grupas	• ekonomiskā situācija vietējā tirgū • ekonomikas tendences vietējā tirgū • ārvalstu ekonomika un tendences • vispārējie nodokļu jautājumi • produktu vai pakalpojumu specifiskie nodokļi • ar sezonalitāti vai laika apstākļiem saistītie jautājumi • tirgus un tirdzniecības cikli • specifiski nozares faktori • tirgus kanāli un izplatīšanas tendences • klientu vai gala lietotāju virzītājspēki • procentu likmes un valūtas kursi
Sociālie faktori	**Tehnoloģiskie faktori**
• dzīves stila tendences • demogrāfija • patērētāju attieksme un uzskati • mediju uzskati • izmaiņas likumdošanā, kas ietekmē sociālos faktorus • zīmola, uzņēmuma, tehnoloģijas veidols • patērētāju iepirkšanās paradumi • mode un atdarināšanas paraugi • svarīgākie notikumi un ietekme • iepirkšanās iespējas un tendences • etniskie vai reliģiskie faktori • reklāma un publicitāte	• konkurējošās tehnoloģijas attīstība • izpētes finansējums • asociētās vai atkarīgās tehnoloģijas • aizstājumu tehnoloģija vai risinājumi • tehnoloģijas brieduma pakāpe • ražošanas briedums un jauda • informācija un komunikācijas • patērētāju iepirkšanās mehānismi vai tehnoloģija • likumdošana tehnoloģiju jomā • inovācijas potenciāls • piekļuve tehnoloģijai, licencēšana, patenti • intelektuālā īpašuma jautājumi

3. att. PEST analīzes modelis

Detalizēts PEST analīzes apraksts atrodams Vikipēdijā[9].

Abas metodes sniedz visaptverošu un strukturētu pārskatu par klientūras vajadzībām. Analīzes rezultāti papildinās biznesa plānu un tādējādi palīdzēs iegūt finansējumu CSIRT izveidei.

Saziņas kanāli

Analīzē ir jāiekļauj tāds svarīgs punkts kā iespējamās saziņas un informācijas izplatīšanas metodes („Kā sazināties ar klientūru?”).

[9] PEST analīze Vikipēdijā: http://en.wikipedia.org/wiki/PEST_analysis

Jāapsver iespējas regulāri apmeklēt klientūru personiski. Praksē ir pierādījies, ka personiska tikšanās atvieglo sadarbību. Ja abas puses vēlas sadarboties, tikšanās palīdzēs izveidot atvērtākas sadarbības attiecības.

Parasti CSIRT izmanto vairākus saziņas kanālus. Šādi kanāli ir pierādījuši savu lietderību praksē, un to izmantošanu būtu vērts apsvērt:

- sabiedriski pieejama tīmekļa vietne,
- slēgta tīmekļa vietnes sadaļa biedriem,
- tīmekļa veidlapas incidentu paziņošanai,
- pasta ziņojumu nosūtīšanas saraksti,
- personalizēts e-pasts,
- telefons vai fakss,
- SMS,
- „parastās" papīra vēstules,
- mēneša vai gada ziņojumi.

Papildus e-pasta, tīmekļa veidlapu, telefona vai faksa izmantošanai, strādājot ar incidentiem (lai saņemtu ziņojumus no klientūras, koordinētu darbu ar citām vienībām vai sniegtu komentārus un atbalstu cietušajam), vairums CSIRT publicē savus konsultatīvos materiālus par drošības jautājumiem publiski pieejamā tīmekļa vietnē vai izsūta tos sarakstā iekļautiem e-pasta adresātiem.

! Ja iespējams, informāciju vajadzētu izplatīt drošā veidā. E-pastu, piemēram, var digitāli parakstīt ar PGP, un konfidenciālu informāciju par incidentiem vienmēr vajadzētu sūtīt šifrētā veidā.

Plašāku informāciju skatīt 8.5. nodaļā „Pieejamie CSIRT rīki". Skatīt arī *RFC2350*[10] 2.3. nodaļu.

Fiktīvā CSIRT (3a. uzdevums)

Klientūras un piemēroto komunikācijas kanālu analizēšana

Piedaloties svarīgākajiem vadības un klientūras pārstāvjiem, ideju ģenerēšanas sesijā tiek iegūta pietiekama informācija SVID analīzei. Analīzes rezultātā tiek secināts, ka nepieciešami šādi pamatpakalpojumi:

- trauksmes ziņojumi un brīdinājumi,
- darbs ar incidentiem (analīze, atbalsts un koordinācija, reaģējot uz incidentu),
- paziņojumi.

Ir jānodrošina, lai informācijas izplatīšana ir labi organizēta, sasniedzot maksimāli lielu klientūras daļu. Tāpēc tiek pieņemts lēmums, ka trauksmes, brīdinājumus un paziņojumus publicēs konsultatīvo drošības materiālu formā specializētā tīmekļa vietnē un izsūtīs sarakstā iekļautiem e-pasta adresātiem. Incidentu ziņojumu saņemšanai CSIRT izmantos arī e-pastu, telefonu un faksu. Vienota tīmekļa veidlapa ir plānota nākamajā solī.

SVID analīzes paraugu skatiet nākošā lappusē.

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

Stiprā puse: • uzņēmuma darbiniekiem ir zināšanas; • viņiem patīk plānot, un tie ir gatavi sadarboties; • atbalsts un finansējums no uzņēmuma valdes.	**Vājā puse:** • nepietiekamais saziņas līmenis starp dažādām nodaļām un filiālēm; • nav koordinācijas IT incidentu gadījumā; • daudz „mazu" nodaļu.
Iespējas: • liela nestrukturētas informācijas plūsma par ievainojamību; • liela nepieciešamība pēc koordinācijas; • incidentu radīto zaudējumu samazināšana; • daudz „vaļēju galu" IT drošības jautājumos; • darbinieku apmācība IT drošības jautājumos.	**Draudi:** • nepietiekams pieejamās naudas daudzums; • nepietiekams darbinieku skaits; • lielas cerības uz sagaidāmo rezultātu; • kultūra.

4. att.

Parauga SVID analīze

5.3.2. Misijas formulējums

Nākamais uzdevums pēc klientūras vajadzību un vēlmju analīzes saistībā ar CSIRT pakalpojumiem ir misijas formulēšana.

Misijas formulējums raksturo organizācijas pamatfunkciju sabiedrībā saistībā ar produktiem un pakalpojumiem, ko tā sniedz klientūrai. Tas dod iespēju skaidri izklāstīt CSIRT pastāvēšanas būtību un funkciju.

Misijas formulējumam vajadzētu būt īsam, bet ne pārāk skopam, jo parasti tas nemainīsies pāris gadus.

Daži funkcionējošu CSIRT misijas formulējumu piemēri:

„<CSIRT nosaukums> sniedz informāciju un palīdzību savai <klientūrai (nodefinējiet savu klientūru)>, realizējot proaktīvus pasākumus, lai samazinātu datoru drošības incidentu risku, kā arī lai reaģētu uz incidentiem, kad tie notiek."

„Sniegt atbalstu <klientūrai>, novēršot IT drošības incidentus un reaģējot uz tiem."[11]

[11] *Govcert.nl* misijas formulējums: http://www.govcert.nl

Misijas formulējums ir ļoti svarīgs un nepieciešams sākuma uzdevums. Detalizētāku aprakstu par informāciju, ko CSIRT vajadzētu publicēt, lūdzu, skatiet *RFC2350*[12] 2.1. nodaļā.

Fiktīvā CSIRT (3b. uzdevums)
Fiktīvās CSIRT vadība ir uzrakstījusi šādu misijas formulējumu: *„Fiktīvā CSIRT sniedz informāciju un palīdzību mītnes organizācijas darbiniekiem, lai samazinātu datoru drošības incidentu risku, kā arī lai reaģētu uz incidentiem, kad tie notiek."* Līdz ar to fiktīvā CSIRT skaidri pasaka, ka tā ir uzņēmuma iekšēja CSIRT un ka tās pamatnodarbošanās ir IT drošības jautājumi.

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

6. Biznesa plāna sastādīšana

Šādi uzdevumi ir izpildīti:

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.
2. Kādam sektoram tiks sniegti jaunās CSIRT vienības pakalpojumi?
3. Kāda veida pakalpojumus CSIRT var sniegt savai klientūrai.
4. Klientūras un vides analīze.
5. Misijas formulēšana

>> Nākamais uzdevums ir biznesa plāna sastādīšana.

Analīzes rezultāti sniedz labu pārskatu par klientūras vajadzībām un vājajām pusēm (pieņemtajām), tāpēc šī informācija tiek izmantota nākamajā uzdevumā.

6.1. Finanšu modeļa definēšana

Pēc analīzes darbības uzsākšanai tika atlasīti daži pamatpakalpojumi. Nākamais uzdevums ir apsvērt finansiālo modeli — kādi sniegto pakalpojumu parametri ir piemēroti un apmaksājami.

Ideālā variantā finansējumu pielāgotu klientūras vajadzībām, bet reālā dzīvē sniedzamo pakalpojumu klāsts ir jāpielāgo piešķirtajam budžetam. Tāpēc reālāk ir sākt ar naudas jautājumu plānošanu.

6.1.1. Izmaksu modelis

Divi galvenie faktori, kas ietekmē izmaksas, ir darba stundas un algoto darbinieku skaits (un kvalitāte). Vai nepieciešams reaģēt uz incidentiem un nodrošināt atbalstu 24 stundas diennaktī visas nedēļās garumā vai šie pakalpojumi tiks sniegti tikai darba laikā?

Atkarībā no vēlamā darba laika un biroja aprīkojuma (vai, piemēram, ir iespējams strādāt no mājām?) var būt izdevīgi strādāt pēc izsaukuma dežūrām vai saskaņā ar plānotām dežūrām.

Varētu domāt arī par abu — proaktīvu un reaktīvu — pakalpojumu sniegšanu darba laikā. Ārpus darba laika tiks piedāvāti tikai ierobežoti pakalpojumi, piemēram, tikai nopietnu katastrofu un incidentu gadījumā, un tos nodrošinās dežurējošs darbinieks pēc izsaukuma.

Vēl viena iespēja ir meklēt starptautiskas sadarbības iespējas ar CSIRT vienībām. Jau pastāv *Following the Sun* (seko saulei) sadarbības piemēri. Piemēram, veiksmīga ir izrādījusies Eiropas un Amerikas vienību sadarbība, kas nodrošina labu iespēju papildināt viena otra kapacitāti. Piemēram, *Sun Microsystems* CSIRT, kam ir daudzas filiāles dažādās laika zonās visā pasaulē (bet tās visas ir vienas CSIRT komandas locekļi) sniedz 24x7 pakalpojumus, komandām no dažādām pasaules vietām, strādājot

maiņās. Tas neietekmē izmaksas, jo vienības strādā tikai parastajās darba stundās, vienlaicīgi sniedzot pakalpojumus „guļošajai pasaules daļai".

Atbilstoši labai praksei 24x7 pakalpojumu nepieciešamību vajadzētu dziļāk izanalizēt ar klientūru. Naktī sniegtiem trauksmes ziņojumiem un brīdinājumiem nav lielas jēgas, ja saņēmējs tos izlasa tikai nākošajā rītā. Robežšķirtni starp „nepieciešamības pēc pakalpojuma" un „vēlēšanās pēc pakalpojuma" ir grūti noteikt, bet, nosakot vajadzīgo darbinieku skaitu un aprīkojumu, jo īpaši darba stundu skaitam ir milzīga nozīme, un tādēļ šis faktors lielā mērā ietekmē izmaksu modeli.

6.1.2. Ienākumu modelis

Kad zināmas izmaksas, saprātīgs tālākais uzdevums būtu domāt par iespējamiem ienākumu modeļiem — kā plānotos pakalpojumus varēs finansēt. Jāizvērtē vairāki iespējamie scenāriji.

Esošo resursu izmantošana
Vienmēr ir lietderīgi izvērtēt jau esošos resursus citās uzņēmuma daļās. Vai piemēroti darbinieki jau tiek algoti (piemēram, pašreizējā IT nodaļa), vai tiem ir vajadzīgā pieredze un speciālās zināšanas? Iespējams, ka ar vadību var vienoties par šo darbinieku norīkošanu darbam CSIRT sākuma posmā vai ka tie var sniegt atbalstu CSIRT pēc vajadzības.

Dalības maksa
Gada vai ceturkšņa dalības maksa ir vēl viena iespēja, kā iekasēt samaksu par pakalpojumiem. Par papildu pakalpojumiem, piemēram, par konsultācijām vai drošības auditiem, samaksu var noteikt atkarībā no to izmantošanas.

Vēl viens apsverams scenārijs — klientūrai uzņēmuma iekšienē pakalpojumi tiek piedāvāti bez maksas, bet ārējiem klientiem sniegtie pakalpojumi ir par maksu. Vēl publiskās tīmekļa vietnēs var publicēt konsultatīvos materiālus un informācijas biļetenus, paredzot „Tikai biedriem" sadaļu, kurā ir specializēta, detalizētāka un klientu vajadzībām vairāk pielāgota informācija.

Praksē ir pierādījies, ka „Parakstīšanās uz CSIRT pakalpojumu" sniedz ierobežotas finansēšana iespējas, īpaši darbības uzsākšanas posmā. Jo, piemēram, pastāv fiksētas darbinieku algošanas un iekārtu izmaksas, kas jāsedz uzreiz. Šādu izmaksu finansēšana, pārdodot CSIRT pakalpojumus ir sarežģīta un prasa ļoti detalizēti finanšu analīzi, lai noskaidrotu „bezzaudējumu punktu".

Subsīdijas
Tā kā mūsdienās vairumā valstu ir IT drošības projektiem paredzēti fondi, vēl viena iespēja ir pieteikties projekta subsidēšanai no valsts vai valsts aģentūras. Iesākumam varētu sazināties ar Iekšlietu ministriju.

Protams, ir iespējams izvēlēties kombinētus realizācijas modeļus.

6.2. Organizācijas struktūras noteikšana

CSIRT organizācijas struktūra lielā mēra ir atkarīga no esošās mītnes organizācijas struktūras un klientūras. Tā ir atkarīga arī no prasmīgu speciālistu pieejamības, ko var algot pastāvīgam darbam vai pēc nepieciešamības konkrētam uzdevumam.

Tipiskā CSIRT vienībā parasti ir šādas pozīcijas:

Vispārējā vadība
- vadītājs

Darbinieki
- biroja vadītājs
- grāmatvedis
- komunikāciju konsultants
- juriskonsults

Operatīvā darba tehniskā vienība
- tehniskās vienības vadītājs
- CSIRT tehniķi, kas sniedz CSIRT pakalpojumus
- pētnieki

Pieaicinātie konsultanti
- algo pēc vajadzības

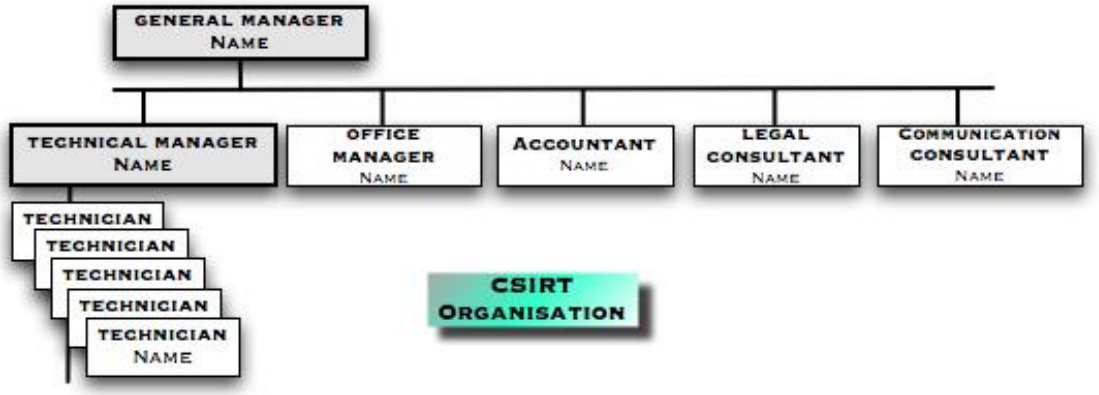
Ir ļoti svarīgi, lai vienībā būtu jurists, īpaši CSIRT darbības uzsākšanas posmā. Tas sadārdzinās izmaksas, bet gala rezultātā aiztaupīs laiku un juridiskas problēmas.

Ja klientūrai ir daudzveidīgas speciālās zināšanas un CSIRT ir plaša atpazīstamība medijos, vienībā ļoti noderīgi ir iesaistīt saziņas speciālistu. Šie speciālisti var veltīt pastiprinātu uzmanību tam, lai pasniegtu tehniski sarežģītus jautājumus klientūrai vai mediju sadarbības partneriem saprotamākā valodā. Turklāt komunikāciju speciālists nodrošinās saikni starp klientūru un tehniskajiem speciālistiem un tādējādi darbosies kā „tulks" vai „koordinators" starp šīm divām grupām.

Tālāk sniegti daži darbojušos CSIRT organizatoriskie modeļi.

6.2.1. Neatkarīga uzņēmuma modelis

CSIRT tiek veidota un darbojas kā neatkarīga organizācija, kurai ir sava vadība un darbinieki.

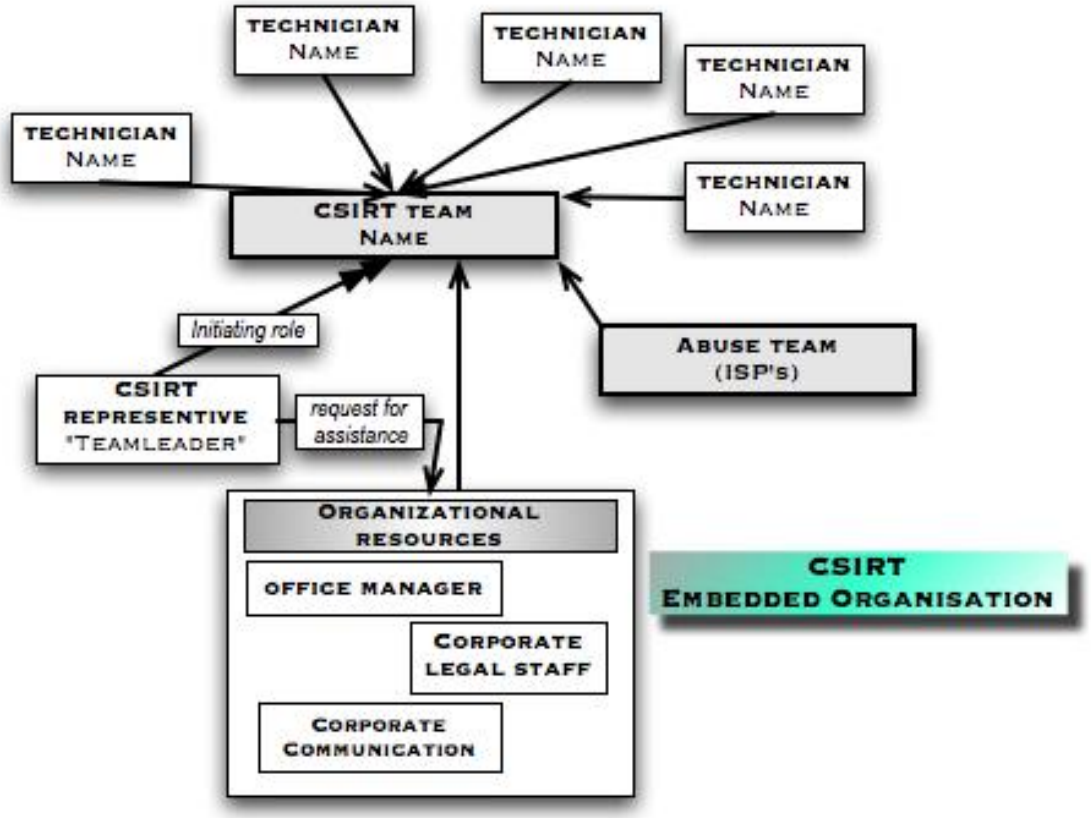


5. att. Neatkarīga uzņēmuma modelis

6.2.2. Iegultais modelis

Šo modeli var izmantot, ja CSIRT ir jāveido esošā organizācijā, piemēram, izmantojot esošu IT nodaļu. CSIRT vada vienības vadītājs, kas ir atbildīgs par CSIRT darbību. Risinot incidentus vai realizējot CSIRT pasākumus, vienības vadītājs pulcē vajadzīgos tehniķus. Lai saņemtu speciālistu atbalstu, vadītājs var lūgt palīdzību no esošās organizācijas.

Šo modeli var pielāgot arī īpašām situācijām, kad tādas izveidojas. Šajā gadījumā vienībai ir piešķirts noteikts pilna darba laika darbinieku ekvivalents (*Full Time Equivalent FTE*). Lai interneta pakalpojumu sniedzējs sniegtu palīdzību ļaunlietošanas gadījumos, vajadzīga pilna laika darba vieta, ko nodrošina viens vai (vairumā gadījumu) vairāki FTE.

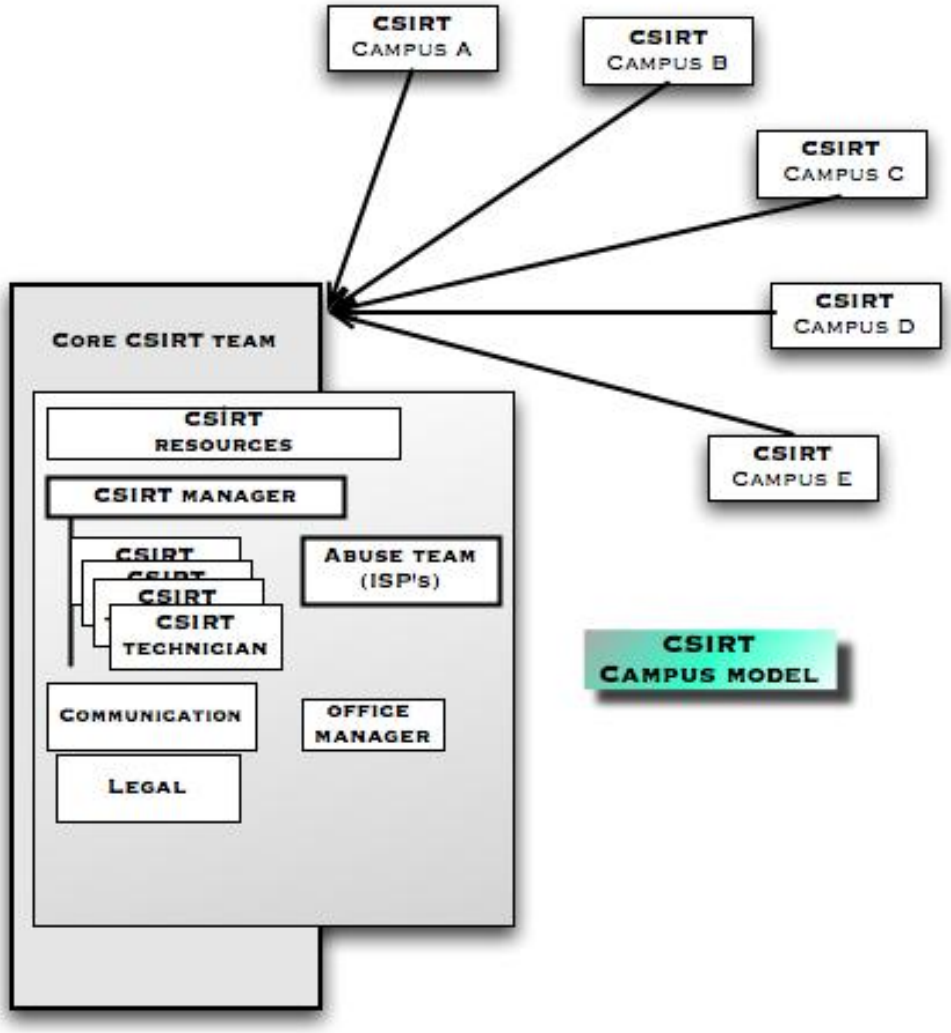


6. att. Iegultais organizācijas modelis

6.2.3. Universitātes pilsētiņas modelis

Kā norāda nosaukums, universitātes pilsētiņas modeli galvenokārt izmanto akadēmisku un izpētes iestāžu CSIRT. Vairumā gadījumu akadēmiskas un izpētes organizācijas veido dažādi universitāšu un universitātes pilsētiņas objekti, kas atrodas vairākās vietās kādā reģionā vai pat visā valstī (kā *NREN*, *National Research Networks* gadījumā). Parasti šīs organizācijas ir viena no otras neatkarīgas, un bieži vien tām ir savas CSIRT vienības. Parasti šīs CSIRT organizatoriski ir apvienotas vienā „mātes" jeb galvenajā CSIRT. Galvenā CSIRT veic koordinēšanu un ir vienīgais kontaktpunkts saziņai ar ārpasauli. Vairumā gadījumu galvenā CSIRT sniedz CSIRT pamatpakalpojumus, kā arī izplata informāciju par incidentiem attiecīgajām universitātes pilsētiņas CSIRT.

Dažas CSIRT vienības sniedz CSIRT pamatpakalpojumus rotēšanas kārtībā, kas samazina galvenās CSIRT pieskaitāmās izmaksas.



7. att. Universitātes pilsētiņas modelis

6.2.4. Brīvprātīgais modelis

Šajā organizācijas modelī apvienojas cilvēku grupa (speciālisti), kas viens otram (un citiem) brīvprātīgi sniedz konsultācijas un atbalstu. Tā ir brīvi formēta kopiena, un tā lielā mērā ir atkarīga no dalībnieku motivācijas.

Šo modeli izmanto, piemēram, WARP kopiena[13].

6.3. Atbilstoša personāla algošana

Kad ir nolemts, kādi pakalpojumi un kāda līmeņa atbalsts tiks nodrošināts un kāds būs organizācijas modelis, nākamais uzdevums ir atrast pietiekamu kvalificētu darbinieku skaitu.

Ir gandrīz neiespējami sniegt konkrētus skaitļus par nepieciešamo tehnisko darbinieku skaitu, bet šādi pamata apsvērumi praksē ir izrādījušies noderīgi:

- Iai sniegtu divus pamatpakalpojumus — izplatītu konsultatīvos biļetenus un strādātu ar incidentiem — vajag vismaz **4** FTE (pilna darba laika ekvivalentus);
- Iai nodrošinātu pilnu CSIRT darbību darba laikā un uzturētu sistēmas: **6** līdz **8** FTE (pilna darba laika ekvivalentus);
- Iai nodrošinātu pilnu 24x7 maiņas darbu (2 maiņas ārpus parastā darba laika), vajag vismaz **12** FTE.

Šie skaitļi ietver arī rezervi slimības gadījumiem, brīvdienām utml. Turklāt vajag pārliecināties, kādi ir vietējā kolektīvā darba līguma nosacījumi. Ja cilvēki strādā ārpus darba laika, tas var radīt papildu izmaksas par virsstundu darbu.

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

Tālāk ir sniegts īss pārskats par CSIRT speciālistu galvenajām prasmēm.

Tehnisko darbinieku darba aprakstu punkti

Personīgās prasmes:
- elastīgs, radošs ar labu komandas izjūtu,
- labas analītiskās prasmes,
- spēja saprotamā valodā izskaidrot sarežģītus tehniskus jautājumus,
- laba izpratne par konfidencialitāti un procesuālu darbu,
- labas organizatora spējas,
- noturība pret stresu,
- labas komunikatīvās un rakstītprasmes,
- atvērtība un gatavība mācīties.

Tehniskā kompetence:
- plašas zināšanas par interneta tehnoloģiju un protokoliem,
- zināšanas par Linux un Unix sistēmām (atkarībā no klientūras iekārtām),
- zināšanas par Windows sistēmām (atkarībā no klientūras iekārtām),
- zināšanas par infrastruktūras aprīkojumu (maršutētāju, komutatoriem, DNS sistēmu, starpniekiekārtām, pastu u.c.),
- zināšanas par interneta lietojumprogrammām (SMTP, HTTP, FTP, telnet, SSH, u.c.),
- zināšanas par drošības draudiem (DDoS, personas datu izmānīšanu, vietnes pārveidošanu, okšķerēšanu u.c.),
- zināšanas par risku vērtēšanu un to praktisko pielietojumu.

Papildu prasmes:
- vēlēšanas strādāt 24x7 režīmā vai pēc izsaukuma (atkarībā no darbības modeļa),
- maksimālais ceļošanas attālums (pieejamība birojā ārkārtas gadījumā; maksimālais ceļā pavadītais laiks),
- izglītības līmenis,
- darba pieredze IT drošības sektorā.

Fiktīvā CSIRT (4. uzdevums)

Biznesa plāna sastādīšana

Finanšu modelis

Tā kā uzņēmums nodrošina 24x7 e-darījumu pakalpojumus un tam ir IT nodaļa, kas strādā 24x7 režīmā, tiek nolemts sniegt pilnus pakalpojumus darba laikā un ārpus parastā darba laika strādāt pēc izsaukuma. Klientūrai pakalpojumi tiks sniegti bez maksas, bet iespēja sniegt pakalpojumus klientiem ārpus uzņēmuma tiks apsvērta izmēģinājuma un novērtēšanas posmā.

Ienākumu modelis

Darbības sākuma un izmēģinājuma posmā CSIRT finansēs mītnes uzņēmums. Izmēģinājuma un novērtēšanas posmā tiks apspriesta papildu finansēšana, ieskaitot iespēju pārdot pakalpojumus klientiem ārpus uzņēmuma.

Organizācijas modelis
Mītnes uzņēmums ir neliels uzņēmums, tāpēc tiek izvēlēts iegultais modelis.
Darba laikā trīs darbinieki sniegs pamatpakalpojumus (izplatīs konsultatīvos drošības materiālus, strādās ar incidentiem un veiks koordinēšanu).

Uzņēmuma IT nodaļa jau nodarbina cilvēkus ar atbilstošām iemaņām. Ar nodaļu tiek panākta vienošanās, ka jaunā CSIRT vienība pēc vajadzības var lūgt tās atbalstu. Turklāt var izmantot tās 2. līmeņa izsaukuma tehniķus.
CSIRT vienībā būs 4 pilna darba laika dalībnieki un 5 papildu dalībnieki. Viens no tiem strādās maiņās rotācijas kārtībā.

Darbinieki
CSIRT vienības vadītājam ir pieredze drošības darbā, sniedzot 1. un 2. līmeņa atbalstu, un viņš ir strādājis krīzes seku likvidēšanas pārvaldības jomā Pārējie trīs vienības dalībnieki ir drošības speciālisti. Nepilnas slodzes CSIRT vienības dalībnieki, kas piesaistīti no IT nodaļas, ir uzņēmuma infrastruktūras speciālisti.

6.4. Biroja telpu un iekārtu izmantošana

Iekārtu, biroja telpu un fiziskā drošība ir ļoti plašas tēmas, tāpēc šajā dokumentā izsmeļošu aprakstu nav iespējams sniegt. Šīs nodaļas nolūks ir sniegt īsu šīs tēmas pārskatu.

Plašāku informāciju par fizisko drošību var atrast:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

„Ēkas nocietināšana"
Tā kā CSIRT parasti strādā ar ļoti slepenu informāciju, vienībai vajadzētu ļaut pašai rūpēties par biroja fizisko drošību. Tas lielā mērā būs atkarīgs no esošajiem objektiem un infrastruktūras un mītnes uzņēmuma informācijas drošības politikas.

Valdības, piemēram, ievieš klasificēšanas programmas un veic striktus pasākumus attiecībā uz rīcību ar konfidenciālu informāciju. Uzziniet no vietējā uzņēmuma vai institūcijas, kādi ir vietējie noteikumi un politika.

Parasti, izzinot vietējos noteikumus, politiku un citus tiesiskos jautājumus, jauna CSIRT ir atkarīga no sadarbības ar mītnes organizāciju.

Izsmeļošs apraksts par visiem pasākumiem, kas nepieciešami attiecībā uz iekārtu un drošību, sniedzas ārpus šī dokumenta ietvariem. Īss CSIRT galveno drošības līdzekļu saraksts ir atrodams tālāk tekstā.

Galvenie noteikumi par ēkas izmantošanu:
- izmantojiet piekļuves kontroli;
- piekļuve CSIRT birojam (vismaz) drīkstētu būt tikai CSIRT darbiniekiem;
- novērojiet birojus un ieejas ar kamerām;
- arhivējiet konfidenciālu informāciju dokumentu skapjos vai seifā;
- izmantojiet drošas IT sistēmas.

Galvenie noteikumi par IT iekārtu izmantošanu:
- izmantojiet iekārtas, ko darbinieki var apkalpot;
- visām sistēmām veiciet drošības pasākumus;
- pirms pieslēgšanas internetam pielabojiet un atjauniniet visas sistēmas;
- izmantojiet drošības programmatūru (ugunsmūrus, daudzkārtējus pretvīrusu skenerus, pretspiegošanas programmas utml.).

Komunikācijas kanālu uzturēšana
- sabiedriski pieejama tīmekļa vietne
- slēgta tīmekļa vietnes sadaļa biedriem
- tīmekļa veidlapas incidentu paziņošanai
- e-pasts (PGP / GPG / S/MIME atbalsts)
- programmatūra pasta nosūtīšanai sarakstā iekļautiem adresātiem
- atsevišķs telefona numurs klientūrai
    - telefons
    - fakss
    - SMS

Uzskaites sistēma vai sistēmas
- kontaktinformācijas datu bāze ar informāciju par vienības dalībniekiem, citām vienībām u.c.
- CRM rīki
- talonu sistēma darbā ar incidentiem

„Korporatīvā noformējuma" izmantošana dokumentos
- standarta e-pasta un konsultatīvo biļetenu noformējums
- „parastās" papīra vēstules
- mēneša vai gada ziņojumi
- incidentu ziņojuma veidlapa

Citi jautājumi
- uzbrukumu gadījumā jāparedz ārkārtas komunikācijas kanāli
- jāparedz rezerve attiecībā uz interneta pieslēguma iespējām

Plašāku informāciju par īpašiem CSIRT rīkiem skatīt 8.5. nodaļā „Pieejamie CSIRT rīki".

6.5. Informācijas drošības politikas formulēšana

Informācijas drošības politika ir atkarīga no CSIRT veida. Politikai ne tikai jāapraksta vēlamie operatīvie un administratīvie procesi un procedūras, bet arī jāatbilst likumdošanai un standartiem, īpaši attiecībā uz CSIRT atbildību. CSIRT parasti ir jāievēro valsts likumi un noteikumi, kas bieži vien tiek īstenoti Eiropas likumdošanas (parasti direktīvu) un citu starptautisko līgumu kontekstā. Standarti ne vienmēr ir jāievēro tieši, bet to ievērošanu var pieprasīt vai ieteikt likumi un noteikumi.

Tālāk tekstā dots īss saraksts ar iespējamiem likumiem un noteikumiem.

Valsts
- dažādi likumi par informācijas tehnoloģiju, telekomunikācijām un medijiem
- likumi par datu un privātuma aizsardzību
- likumi un noteikumi par datu saglabāšanu
- likumi par finansēm, grāmatvedību un uzņēmumu vadīšanu
- uzņēmumu pārvaldības un IT pārvaldības ētikas kodeksi

Eiropas
- direktīva par elektroniskajiem parakstiem (1993/93EK)
- direktīvas par datu (1995/46/EK) un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (2002/58/EK)
- direktīvas par elektroniskajiem komunikāciju tīkliem un pakalpojumiem (2002/19/EK – 2002/22/EK)
- direktīvas par uzņēmējdarbības tiesībām (piemēram, 8. uzņēmumtiesību direktīva)

Starptautiskie likumi
- Bāzeles II nolīgums (īpaši attiecībā uz operatīvo risku pārvaldību)
- Eiropas Padomes Konvencija par kibernoziegumiem
- Eiropas Padomes Konvencija par cilvēktiesībām (8. pants par privātumu)
- starptautiskie grāmatvedības standarti (IAS, tie zināmā mērā nosaka IT kontroli)

Standarti
- Britu standarts BS 7799 (informācijas drošība)
- starptautiskie standarti ISO2700x (informācijas drošības pārvaldības sistēmas)
- vācu IT-*Grundschutzbuch*, franču *EBIOS* un citu valstu varianti

Lai noskaidrotu, vai CSIRT darbojas saskaņā ar valsts un starptautiskajiem likumiem, lūdzu, konsultējieties ar savu juriskonsultu.

Pamatjautājumi, uz kuriem drošības politikai vajadzētu rast atbildes ir šādi:

- Ka tiek kodēta vai klasificēta ienākošā informācija?
- Kā informācija tiek apstrādāta, īpaši attiecībā uz ekskluzīvām piekļuves tiesībām?
- Kādi apsvērumi tiek ņemti vērā, izpaužot informāciju, īpaši, ja ar incidentu saistīta informācija tiek sniegta citām vienībām vai struktūrām?
- Vai, strādājot ar informāciju, ir jāņem vērā juridiski apsvērumi?

- Vai pastāv noteikumi par šifrēšanas izmantošanu, lai aizsargātu ekskluzīvas piekļuves tiesības un neaizskaramību arhivos un/vai datu pārraidi, īpaši ar e-pastu?
- Vai tiesas prāvu gadījumos šī politika paredz iespējamus juridiskos nosacījumus, kā šifratslēgas uzticējumglabāšanu vai atšifrēšanas piemērošanu.

Fiktīvā CSIRT (5. uzdevums)
Biroja iekārtas un izvietojums Tā kā mītnes organizācijai jau ir efektīva fiziskā drošība, šai ziņa jaunā CSIRT ir labi sagatavota. Ir atvēlēta tā saucamā „kara telpa", lai ārkārtas gadījumos varētu veikt koordinēšanu. Šifrēto materiālu un slepeno dokumentu glabāšanai ir iegādāts seifs. Ir iekārtota atsevišķa telefona līnija ar komutatoru kārstās līnijas vajadzībām darba laikā un mobilais telefons ar tādu pašu numuru izsaukumiem ārpus parastā darba laika. Lai paziņotu ar CSIRT saistītu informāciju, var izmantot arī esošo aprīkojumu un uzņēmuma tīmekļa vietni. Tiek izveidots un uzturēts adresātu saraksts ar ierobežotu daļu saziņai ar vienības dalībniekiem un citām vienībām. Visa darbinieku kontaktinformācija tiek glabāta datu bāzē, izdruka atrodas seifā. **Noteikumi** Tā kā CSIRT strādā uzņēmuma ietvaros, kurā jau pastāv informācijas drošības politika, attiecīgie CSIRT drošības noteikumi tiek izveidoti ar uzņēmuma juriskonsulta palīdzību.

6.6. CSIRT un iespējamo valsts iniciatīvu sadarbības iespēju noskaidrošana

Dokumentā jau vairākkārt pieminēts, ka var būt citas CSIRT iniciatīvas un ka ar tām ļoti ieteicams sadarboties. Vajadzētu pēc iespējas drīzāk sazināties ar citām CSIRT vienībām, lai izveidotu kontaktus ar CSIRT kopienām. Parasti citas CSIRT vienības labprāt palīdz jaunām vienībām uzsākt darbu.

ENISA „Uzskaite par CERT aktivitātēm Eiropā"[14] ir labs sākumpunkts, meklējot valstī esošās CSIRT vienības vai CSIRT sadarbības iespējas.

Lai saņemtu palīdzību, meklējot piemērotu informācijas avotu par CSIRT, sazinieties ar ENISA speciālistiem CSIRT jomā:

CERT-Relations@enisa.europa.eu

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

Tālāk sniegts pārskats par CSIRT kopienas aktivitātēm. Izsmeļošāku aprakstu un plašāku informāciju skatīt „Uzskaitē".

Eiropas CSIRT iniciatīva

TF-CSIRT[15]
TF-CSIRT darba grupa veicina sadarbību starp Eiropas datoru drošības incidentu reaģēšanas vienībām (CSIRT). Darba grupas galvenais uzdevums ir nodrošināt forumu pieredzes un zināšanu apmaiņai, izveidot izmēģinājuma projektus Eiropas CSIRT vienību vajadzībām un palīdzēt izveidot jaunas CSIRT vienības.

Darba grupas galvenie uzdevumi:
- nodrošināt forumu pieredzes un zināšanu apmaiņai;
- izveidot izmēģinājuma projektus Eiropas CSIRT vienību vajadzībām;
- veicināt vienotu standartu un procedūru izmantošanu reaģēšanai uz drošības incidentiem;
- palīdzēt jaunu CSIRT vienību izveidē un to darbinieku apmācībā;
- atbilstoši savas kompetences ietvariem, ko 2004. gada 15. septembrī apstiprināja TERENA Tehniskā komiteja, TF-CSIRT darbība galvenokārt aptver Eiropu un tās kaimiņvalstis.

Globālā CSIRT iniciatīva

FIRST[16]
Darbā ar incidentiem FIRST ir vadoša organizācija un atzīts pasaules mēroga līderis. Kļūstot par FIRST biedriem, incidentu reaģēšanas vienības var efektīvāk cīnīties ar drošības incidentiem – veicot gan reaģēšanas, gan proaktīvus pasākumus.

FIRST pulcē vienkopus dažādas datoru drošības incidentu reaģēšanas vienības no valsts, komerciālām un izglītības organizācijām. FIRST mērķis ir sekmēt sadarbību un koordināciju incidentu novēršanas jomā, veicināt spēju ātri reaģēt uz incidentiem un rosināt informācijas apmaiņu tās biedru vidū un visas kopienas ietvaros.

Papildus uzticības tīklam, ko FIRST veido globālajā incidentu reaģēšanas kopienā, FIRST sniedz arī papildvērtības pakalpojumus.

Fiktīvā CSIRT (6. uzdevums)
Sadarbības iespēju meklēšana Izmantojot ENISAS uzskaiti, valstī ātri tiek atrastas dažas CSIRT vienības, un ar tām tiek nodibināti kontakti. Tiek panākta vienošanās, ka vienu no tām apmeklēs tikko darbā pieņemtais vienības vadītājs. Viņš uzzināja par CSIRT aktivitātēm valstī un apmeklēja vienu sapulci. Sapulcē apskatītie darba metožu paraugi un dažu citu vienību piedāvātā palīdzība bija ļoti noderīga.

[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. Biznesa plāna virzīšana

Līdz šim izpildīti šādi uzdevumi:

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.
2. Kādam sektoram tiks sniegti jaunās CSIRT vienības pakalpojumi?
3. Kāda veida pakalpojumus CSIRT var sniegt savai klientūrai.
4. Klientūras un vides analīze
5. Misijas formulēšana
6. Biznesa plāna sastādīšana
    a. finanšu modeļa definēšana
    b. organizācijas struktūras noteikšana
    c. darbinieku pieņemšana
    d. biroja telpas un iekārtas
    e. informācijas drošības politikas formulēšana
    f. sadarbības partneru meklēšana

>> Nākamais uzdevums ir sastādīt projektā plānu, izmantojot iepriekš minētos punktus, un sākt darbu!

Projekta definēšanu var sākt ar darbības ekonomisko pamatojumu. Darbības pamatojums tiek izmantots par projekta plāna pamatu un arī, lai gūtu vadības atbalstu un panāktu līdzekļu vai citu resursu piešķiršanu.

Lai vadība labi apzinātos IT drošības problēmas un tādējādi CSIRT darbs nepārtraukti tiktu atbalstīts, ir svarīgi vadību pastāvīgi informēt.

Darbības pamatojumu sāk ar problēmu un iespēju analīzi, izmantojot kādu no 5.3. nodaļā *Klientūras analīze* aprakstītajiem analīzes modeļiem un meklējot ciešus kontaktus ar potenciālo klientūru.

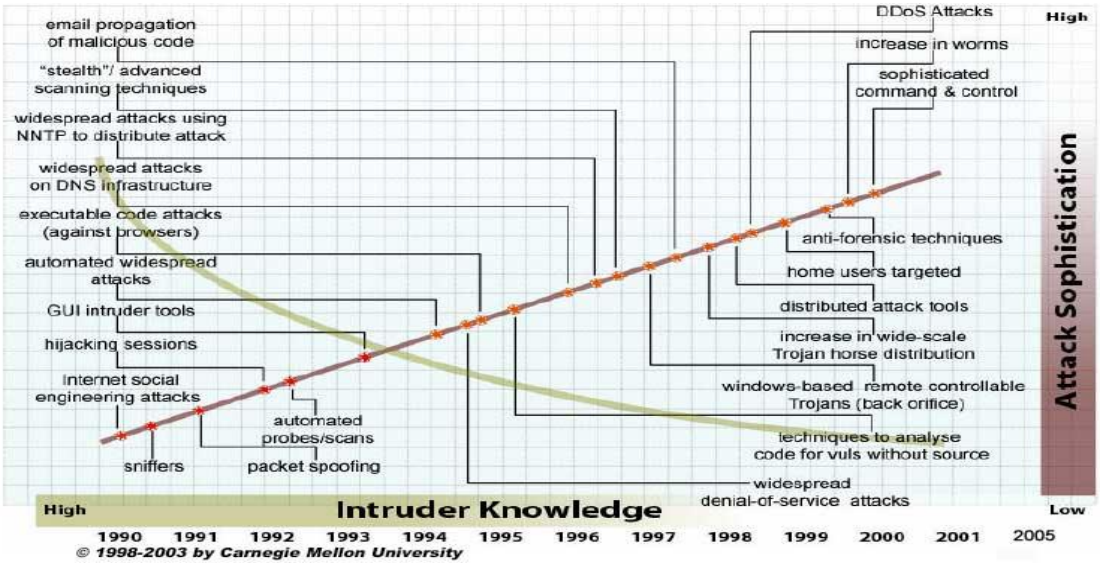
Kā aprakstīts iepriekš, veidojot CSIRT, ir jāpārdomā daudzi jautājumi. Iepriekš minēto materiālu ir jāpielāgo konkrētajām CSIRT vajadzībām atbilstoši to attīstībai.

Ziņojot vadībai, vajadzētu iesniegt pēc iespējas jaunāku informāciju, izmantojot pēdējos laikrakstu vai interneta materiālus, un izskaidrot, kāpēc CSIRT darbam un incidentu iekšējai koordinēšanai ir izšķirīga nozīme, gādājot par uzņēmuma īpašumu drošību. Turklāt ir jāpaskaidro, ka IT jomā tikai pastāvīgs atbalsts var nodrošināt stabilu darbību, īpaši tādā gadījuma, ja uzņēmuma vai institūcijas darbs ir atkarīgs no IT.

(To ilustrē labi zināmais Brūsa Šnaiera (*Bruce Schneier*) izteikums: *„Drošība nav rezultāts, bet gan process[17]!“*)

Pazīstams uzskates līdzeklis, kas ilustrē drošības problēmas, ir CERT/CC sniegtā diagramma:

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



8. att. Iebrucēju zināšanas pret iebrukumu sarežģītību (avots CERT-CC[18])

Tā uzskatāmi attēlo IT drošības tendences, īpaši to, ka arvien izsmalcinātāku uzbrukumu īstenošanai vajag arvien mazākas prasmes.

Vēl jāpiemin tas, ka pastāvīgi samazinās laiks, kas paiet no brīža, kad kļūst pieejami pret ievainojamību vērsti programmatūras atjauninājumi un pret tiem vērsti uzbrukumi.

Uzlabot-> izmantot		**Izplatīšanās ātrums**	
Nimda:	11 mēneši	Code red:	dienas
Slammer:	6 mēneši	Nimda:	stundas
Nachi:	5 mēneši	Slammer:	minūtes
Blaster:	3 nedēļas		
Witty:	1 diena (!)		

Savāktie dati par incidentiem, informācija par iespējamiem uzlabojumiem un gūtajām mācībām arī ir prezentācijai noderīgi materiāli.

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

7.1. Biznesa plāna apraksts un vadības rosinātāji

Vadības iepazīstināšana ar CSIRT un tās idejas popularizēšana pati par sevi neveido biznesa pamatojumu, bet ja šie pasākumi tiek veikti pienācīgā veidā, tie vairumā gadījumu nodrošinās vadības atbalstu CSIRT. No otras puses, idejas pamatošanu nevajadzētu uzskatīt tikai par vadībai domātu pasākumu. To vajadzētu izmantot arī saziņā ar darbiniekiem un klientūru. Termins „darbības ekonomiskais pamatojums" var izklausīties ļoti komerciāls un tāls no CSIRT ikdienas prakses, taču, veidojot CSIRT, tas palīdz koncentrēties un virzīt darbību.

Atbildes uz tālāk uzdotajiem jautājumiem var izmantot, lai izstrādātu labu darbības pamatojumu (minētie piemēri ir hipotētiski un tiek izmantoti tikai ilustrācijai. „Īstās" atbildes lielā mērā ir atkarīgas no „reālajiem" apstākļiem).

- Kāda ir problēma?
- Ko jūs gribētu sasniegt darbā ar klientūru?
- Kas notiks, ja nekas netiks darīts?
- Kas notiks, ja tiks veikti pasākumi?
- Cik tas maksās?
- Kas tiks iegūts?
- Kad sākt un kad tas tiks pabeigts?

Kāda ir problēma?
Vairumā gadījumu ideja par CSIRT izveidi rodas, kad IT kļūst par uzņēmuma vai institūcijas pamatdarbības būtisku sastāvdaļu un kad IT drošības incidenti apdraud uzņēmumam vai institūcijas darbību, padarot drošības risku mazināšanu par ikdienas darbu.

Vairumam uzņēmumu un institūciju parasti ir atbalsta nodaļa vai dienests, bet lielākajā daļā gadījumu incidentiem netiek veltīta pietiekama uzmanība, un rīcība nav pietiekami organizēta. Vairumā gadījumu darbā ar drošībās incidentiem vajadzīgas īpašas prasmes un vērība. Ieguvums būs arī no organizētākas pieejas, kas samazinās darbības risku un uzņēmumam nodarītos zaudējumus.

Lielākajā daļā gadījumu trūkst koordinācijas un darbā ar incidentiem netiek izmantotas esošās zināšanas, kas kopumā varētu novērst nākotnes incidentus, finansiālus zaudējumus un/vai kaitējumu institūcijas reputācijai.

Kādi mērķi sasniedzami darbā ar klientūru?
Kā paskaidrots iepriekš, CSIRT sniegs pakalpojumus klientūrai un palīdzēs klientiem tikt galā ar IT drošības incidentiem un problēmām. Papildu mērķi ir celt zināšanu līmeni IT drošības jomā un izveidot kultūru, kas apzinās drošības svarīgumu.

Šāda kultūra gādā par proaktīvu un preventīvu pasākumu veikšanu jau pašā sākotnē un tādējādi samazina darbības izmaksas.

Sadarbības un palīdzības kultūras ieviešana uzņēmumā vai institūcijā daudzos gadījumos var stimulēt efektivitāti kopumā.

Kas notiks, ja nekas netiks darīts?
Nestrukturēta pieeja darbam ar IT drošību var nākotnē izraisīt zaudējumus, nemaz nerunājot par kaitējumu iestādes reputācijai. Citas iespējamās sekas ir finansiāli zaudējumi un juridiski sarežģījumi.

Kas notiks, ja tiks veikti pasākumi?
Veidosies lielāka izpratne par drošības problēmu atgadījumiem. Tas palīdzēs tos atrisināt efektīvāk un novērsis zaudējumus nākotnē.

Cik tas maksās?
Atkarībā no organizācijas modeļa, izmaksas ietvers CSIRT darbinieku un vadības algas, iekārtu, aprīkojuma un programmatūras licenču izmaksas.

Kas tiks iegūts?
Atkarībā no iepriekšējās darbības un zaudējumiem tiks panākta lielāka procedūru un drošības prakses caurskatāmība, tādējādi aizsargājot būtiskus uzņēmuma īpašumus.

Kāds ir kalendārais grafiks?
Projekta plāna parauga aprakstu skatīt 12. nodaļā *Projekta plāna apraksts*.

Esošo darbības pamatojumu un pieeju piemēri
Šeit atrodami CSIRT darbības pamatojumu piemēri, ar ko vērts iepazīties:

- http://www.cert.org/csirts/AFI_case-study.html
  Finanšu institūcijas CSIRT izveide — gadījuma izpēte.

  Šī dokumenta nolūks ir dalīties ar pieredzi, ko, izstrādājot un ieviešot drošības problēmu risināšanas un datoru drošības incidentu reaģēšanas vienības izveides plānu, guvusi finanšu institūcija (tālāk tekstā – „AFI").

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  CERT POLSKA darbības pamatojuma kopsavilkums (slaidrāde PDF formātā).

- http://www.auscert.org.au/render.html?it=2252
  Incidentu reaģēšanas vienības (IRT) izveide 20. gs. 90. gados bija sarežģīts uzdevums. Daudziem no IRT izveidē iesaistītajiem cilvēkiem nebija iepriekšējas pieredzes. Šajā dokumentā aplūkots, kāda nozīme kopienā var būt IRT un kādi jautājumi jārisina gan darbības organizēšanas laikā, gan pēc tās uzsākšanas. Šī informācija varētu noderēt esošām IRT vienībām, jo tā palīdz izprast iepriekš neskartus jautājumus.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Informācijas drošības, uzņēmuma drošības gadījuma izpēte. Autors: Rodžers Bentons (*Roger Benton*)

  Šajā praktiskajā materiālā tiek apskatīts gadījums, kad apdrošināšanas uzņēmums pāriet uz drošības sistēmu, kas aptver visu uzņēmumu. Šī praktiskā materiāla nolūks ir norādīt, kāds ceļš ejams, veidojot drošības sistēmu vai pārejot uz citu drošības sistēmu. Sākumā piekļuve uzņēmuma datiem tika kontrolēta tikai ar primitīvas tiešsaistes sistēmas palīdzību. Pastāvēja būtisks risks — ārpus tiešsaistes vides nebija nekādu datu neaizskaramības kontroles iespēju. Jebkurš, kam bija programmēšanas pamatiemaņas varēja pievienot, mainīt un/vai dzēst datus.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Marriott e-drošības stratēģija — uzņēmuma-IT sadarbība

  Pēc Krisa Zoladza (*Chris Zoladz, Marriott International*) pieredzes e–darījumu drošība ir process, nevis projekts. Tieši to Zoladzs pavēstīja nesenajā Bostonas e-drošības konferencē un izstādē, ko sponsorēja *Intermedia Group*. Zoladzs ir *Marriott* uzņēmuma informācijas aizsardzības priekšsēdētāja vietnieks, kas strādā juridiskās nodaļas pakļautībā, kaut arī nav jurists. Viņa uzdevums ir noteikt, kur tiek glabāta *Marriott* uzņēmuma pati vērtīgākā darījumu informācija un kā tā pārvietojas uzņēmuma iekšienē un ārpus tā. *Mariott* ir noteicis atsevišķu atbildības sfēru tehniskajai infrastruktūrai, kas atbalsta drošību, kura nodota IT drošības arhitekta ziņā.

Fiktīvā CSIRT (7. uzdevums)
Biznesa plāna virzīšana Tiek nolemts apkopot faktus un skaitļus par uzņēmuma vēsturi. Tas sniedz ļoti noderīgu statistisku pārskatu par IT drošības situāciju. Šo apkopojumu vajag turpināt pēc CSIRT izveides, lai šo statistiku aktualizētu. Tiek nodibināti sakari ar citām CSIRT valstī, lai apspriestu to darbības pamatojumus. Vienības sniedz atbalstu, izveidojot slaidus ar informāciju par jaunākajiem notikumiem IT drošības incidentu jomā un incidentu radītajām izmaksām. Šajā izdomātās CSIRT vienības piemērā nebija aktuālas vajadzības pārliecināt vadību par IT nozares svarīgumu, un tāpēc gūt atbalstu pirmā posma uzsākšanai nebija grūti. Tiek sagatavots darbības pamatojums un projekta plāns, ieskaitot vienības izveides izmaksu aprēķinu un darbības izmaksas.

8. Operatīvo un tehnisko procedūru piemēri (darbplūsmas)

Līdz šim izpildīti šādi uzdevumi:

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.
2. Kādam sektoram tiks sniegti jaunās CSIRT vienības pakalpojumi?
3. Kāda veida pakalpojumus CSIRT var sniegt savai klientūrai.
4. Klientūras un vides analīze.
5. Misijas formulēšana.
6. Biznesa plāna sastādīšana.
   a. Finanšu modeļa definēšana.
   b. Organizācijas struktūras noteikšana.
   c. Darbinieku pieņemšana.
   d. Biroja telpas un iekārtas.
   e. Informācijas drošības politikas formulēšana.
   f. Sadarbības partneru meklēšana.
7. Biznesa plāna virzīšana.
   a. Darbības pamatojuma apstiprināšanas panākšana.
   b. Visu punktu apkopošana projekta plānā.

>> Nākamais uzdevums — sākt CSIRT darbību

Labi izstrādātu darbplūsmu ieviešana uzlabo kvalitāti un samazina vienam incidentam vai ievainojamības gadījumam atvēlēto laiku.

Kā aprakstīts iepriekšējos piemēros, fiktīvā CSIRT ietvers šādus galvenos CSIRT pamatpakalpojumus:

- trauksmes paziņojumus un brīdinājumus,
- darbu ar incidentiem,
- paziņojumus.

Šajā nodaļā sniegti darbplūsmu paraugi, kas raksturīgi CSIRT pamatpakalpojumiem. Šajā nodaļa ir arī informācija par informācijas ievākšanu no dažādiem avotiem, tās svarīguma un autentiskuma pārbaudi un tās tālāku izplatīšanu klientūrai. Visbeidzot nodaļā ir sniegti piemēri par pašām vienkāršākajām procedūrām un konkrētiem CSIRT rīkiem.

8.1. Klientūras instalāciju bāzes novērtējums

Pirmais uzdevums ir izveidot pārskatu par IT sistēmām, kas instalētas jūsu klientūrai. Tādā veidā CSIRT var novērtēt ienākošās informācijas būtiskumu un filtrēt to pirms tālākas izplatīšanas, lai klientūra netiktu pārslogota ar būtībā bezjēdzīgu informāciju.

Sākumā varētu, piemēram, izmantot vienkāršu Excel izklājlapu:

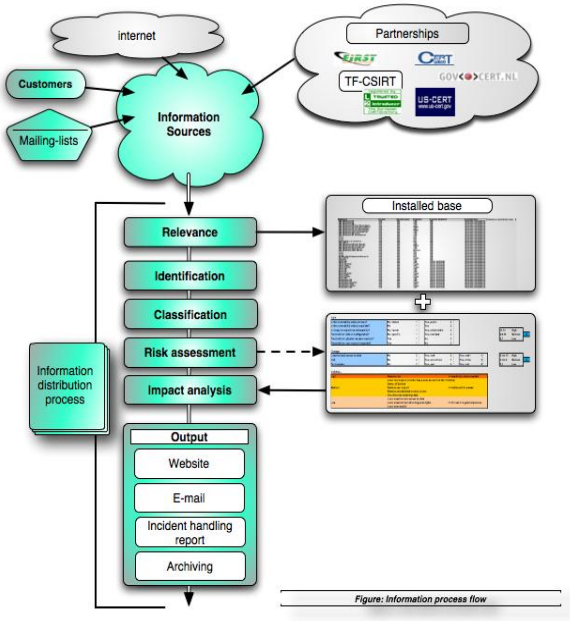
Kategorija	Pielietojums	Programmatūras produkts	Versija	OS	OS versija	Klientūra
Darbvirsma	Birojs	Excel	x-x-x	Microsoft	XP-prof	A
Darbvirsma	Pārlūks	IE	x-x-	Microsoft	XP-prof	A
Tīkls	Maršutētājs	CISCO	x-x-x	CISCO	x-x-x	B
Serveris	Serveris	Linux	x-x-x	L-distro	x-x-x	B
Pakalpojumi	Web serveris	Apache		Unix	x-x-x	B

Izmantojot Excel filtra funkciju, var viegli izvēlēties attiecīgo programmu, lai redzētu, kādu programmatūru katrs klientūras pārstāvis izmanto.

8.2. Trauksmes ziņojumu, brīdinājumu un paziņojumu sastādīšana

Veidojot trauksmes ziņojumus, brīdinājumus un paziņojumus, darbplūsma ir vienāda:

- informācijas ievākšana
- informācijas būtiskuma un izcelsmes avota novērtēšana
- riska novērtēšana, balstoties uz savākto informāciju
- informācijas izplatīšana



9. att. Informācijas analīzes process

Šī darbplūsma tiks detalizētāk aprakstīta nākamajās rindkopās.

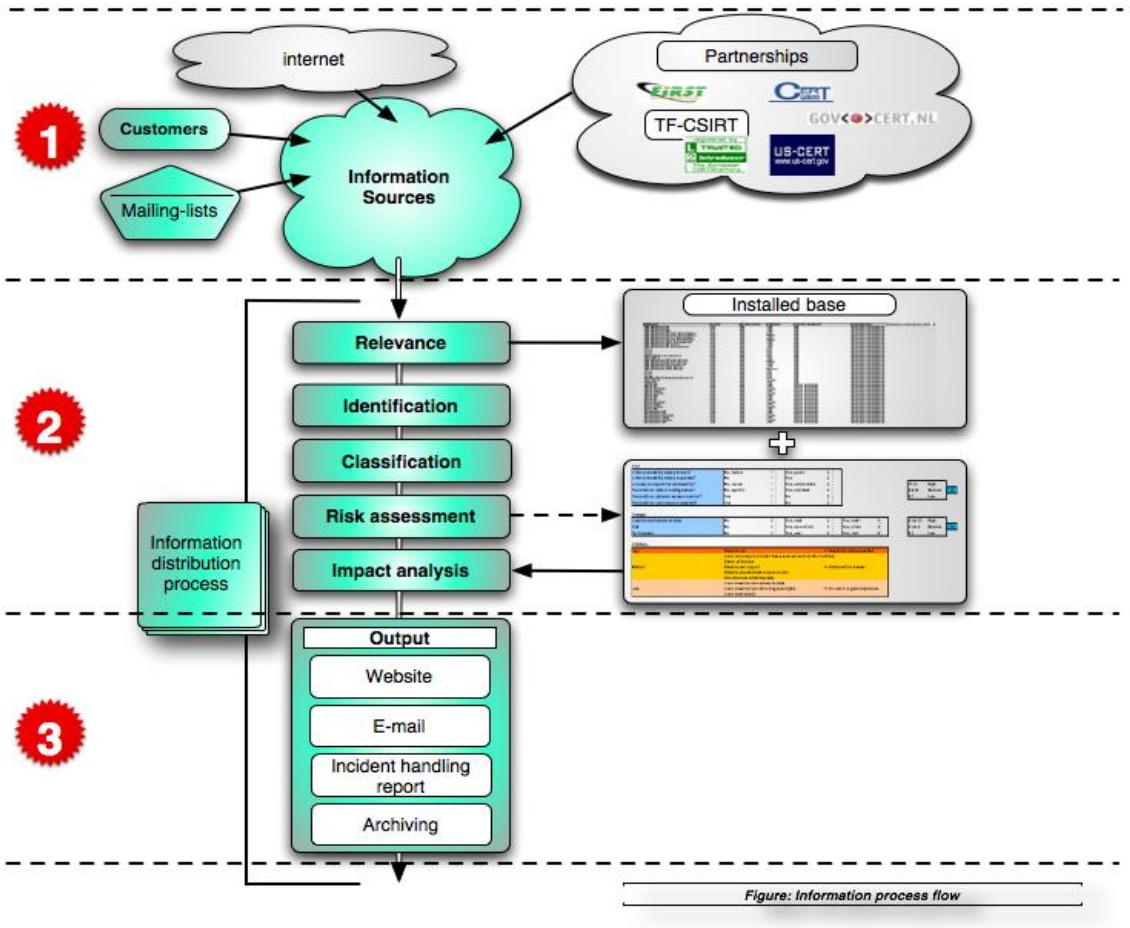


Figure: Information process flow

1. uzdevums — informācijas ievākšana par ievainojamību

Parasti ir divi galvenie informācijas avotu veidi, kas sniedz izejmateriālu piedāvātajiem pakalpojumiem:

- ievainojamības informācija, par (jūsu) IT sistēmām,
- incidentu ziņojumi.

Atkarībā no uzņēmuma darbības veida un IT infrastruktūras ir pieejami vairāki publiski un slēgti informācijas avoti par ievainojamību:

- publiskie un slēgtie adresātu saraksti
- tirgotāju informācija par produktu ievainojamību
- tīmekļa vietnes
- informācija internetā (Google u.c.)
- publiskas un privātas partnerības, kas sniedz informāciju par ievainojamību (FIRST, TF-CSIRT, CERT-CC, US-CERT uc.)

Visa šī informācija papildina zināšanas par konkrētām IT sistēmu ievainojamībām.

Kā minēts iepriekš, daudzi un viegli pieejami informācijas avoti par drošību ir atrodami internetā. ENISA ad-hoc darba grupa „CERT pakalpojumi" publicēja visaptverošu informācijas sarakstu par 2006. gadu.[19].

2. uzdevums — informācijas un riska novērtēšana

Šā uzdevuma mērķis ir izveidot analīzi par konkrētas ievainojamības ietekmi uz klientūras IT infrastruktūru.

Identificēšana
Ienākošā informācija par ievainojamību vienmēr ir jāidentificē pēc tās izcelsmes avota, un pirms informācijas nodošanas klientūrai ir jānoskaidro, vai šis avots ir ticams. Pretējā gadījumā var tikt sacelta viltus trauksme, kas var radīt nevajadzīgu uzņēmuma darba procesu traucējumu un galu galā sabojāt CSIRT reputāciju.

[19] *Ad-hoc* darba grupas CERT pakalpojumi:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Šī procedūra ir piemērs tam, kā tiek noteikts ziņojuma autentiskums.

Procedūra ziņojuma autentiskuma un avota noteikšanai

Galveni kontroljautājumi
1. Vai avots ir zināms un attiecīgi reģistrēts?
2. Vai informācija saņemta pa parasto kanālu?
3. Vai informācija ir „dīvaina", vai ir „sajūta", ka kauts kas nav kārtībā?
4. Uzticieties sev, ja ir šaubas, pārbaudiet vēlreiz!

Pa e-pastu sūtīta informācija
1. Vai avota adrese organizācijai ir pazīstama un vai tā ir informācijas avotu sarakstā?
2. Vai PGP paraksts ir pareizs?
3. Šaubu gadījumā pārbaudiet visu ziņojuma galveni.
4. Rodoties šaubām, pārbaudiet sūtītāja domēnu ar „nslookup" vai „dig"[20].

WWW avoti
1. Pieslēdzoties nodrošinātai tīmekļa vietnei (https ://), pārbaudiet pārlūka sertifikātus.
2. Pārbaudiet avota saturu un derīgumu (tehniski).
3. Šaubu gadījumā neklikšķiniet uz saitēm un nelejupielādējiet programmatūru.
4. Ja rodas šaubas, veiciet domēna „lookup" un „dig" un „traceroute".

Telefons
1. Uzmanīgi ieklausieties runātāja vārdā.
2. Vai balss ir pazīstama?
3. Ja rodas šaubas, palūdziet zvanītāja telefona numuru un palūdziet atļauju atzvanīt.

10. att. Informācijas identificēšanas procedūras piemērs

Būtiskums
Iepriekš izveidoto pārskatu par instalēto aparatūru un programmatūru var izmantot, lai filtrētu ienākošās ievainojamības informācijas būtiskumu ar mērķi atbildēt uz šādiem jautājumiem: „Vai klientūra izmanto šo programmatūru?"; „Vai šī informācija ir viņiem būtiska?"

Klasifikācija
Daļu no saņemtās informācija var klasificēt vai kodēt kā ierobežotu (piemēram, no citām vienībām saņemtos ziņojumus par incidentiem). Informācija ir jāapstrādā atbilstoši nosūtītāja prasībām un uzņēmuma paša informācijas drošības politikai. Labs pamatnoteikums ir: *„Neizplatīt informāciju, ja nav skaidrs, ka tā tam paredzēta; šaubu gadījumā lūdziet nosūtītāja atļauju to darīt".*

[20] Identitātes pārbaudes rīki CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Riska novērtējums un ietekmes analīze
Ievainojamības (potenciālas) riska un ietekmes novērtēšanai ir vairākas metodes.

Risks tiek definēts kā iespējamība izmantot ievainojamību. Ir vairāki svarīgi faktori, tostarp:

- Vai ievainojamība ir zināma?
- Vai ievainojamība ir plaši izplatīta?
- Vai ievainojamību var viegli izmantot?
- Vai ievainojamību var izmantot, iedarbojoties attāli?

Šie jautājumi rada labu izpratni par ievainojamības nopietnību.
Ļoti vienkārša riska aprēķināšanas metode ir šī formula:

Ietekme = risks x iespējamie zaudējumi

Iespējamie zaudējumi var būt šādi:

- nesankcionēta piekļuve datiem,
- darbības liegšana (DOS),
- atļauju ieguve vai pagarināšana.

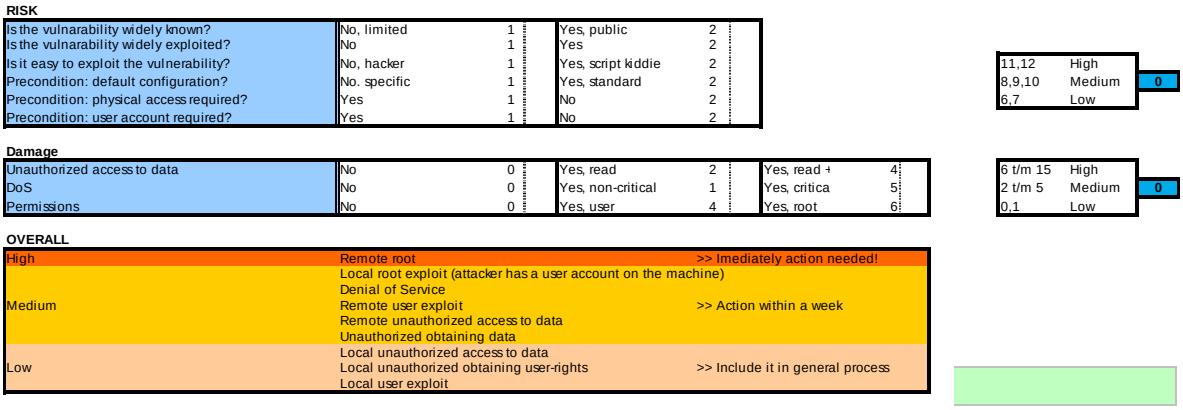
(Sīkākas klasifikācijas shēmas skatīt nodaļas beigās).

Kad šie jautājumi atbildēti, konsultatīvajam materiālam var piešķirt kopējo kategoriju, informējot par iespējamo risku un zaudējumiem. Bieži vien izmanto vienkāršas kategorijas, kā ZEMA, VIDĒJA un AUGSTA.

Ir arī citas, plašākās risku novērtēšanas shēmas.

GOVCERT.NL klasifikācijas shēma[21]

Holandes valdības CSIRT GOVCERT.NL ir izstrādājusi riska novērtēšanas matricu, kuras izveide tika uzsākta Govcert.nl sākuma posmā un kas joprojām tiek papildināta ar jaunākajām tendencēm.



11. att. GOVCERT.NL klasifikācijas shēma

EISPP Common Advisory Format Description (kopējais konsultatīvo materiālu formāta apraksts)[22]

Eiropas Informācijas drošības veicināšanas programma (EISPP) ir projekts, ko Eiropas Kopiena līdzfinansē piektās pamatprogrammas ietvaros. EISPP mērķis ir izveidot Eiropas tīklu, lai ne tikai dalītos ar zināšanām drošības jomā, bet arī lai definētu drošības informācijas saturu un tās izplatīšanas veidus MVU. Sniedzot nepieciešamos IT drošības pakalpojumus, tiks stimulēta Eiropas MVU uzticība e-darījumiem un tās izmantošana, kas radīs plašākas un labākas iespējas veikt jaunus darījumus. ESPP ir Eiropas Komisijas pirmais projekts, kas realizē tās vīziju par Eiropas speciālistu tīkla izveidi Eiropas Savienībā.

DAF *Deutsches Advisory Format* (Vācijas konsultatīvo materiālu formāts)[23]

DAF ir vācu CERT-Verbund (CERT apvienības) iniciatīva, un tā veido pamata elementu dažādu vienību drošības konsultatīvo materiālu izstrādes un izplatīšanas infrastruktūrai. DAF ir pielāgota vācu CERT vajadzībām; standartu ir izstrādājusi un uztur CERT-Bund, DFN-CERT, PRESECURE un Siemens-CERT.

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

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

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

3. uzdevums — informācijas izplatīšana

CSIRT var izvēlēties atšķirīgas izplatīšanas metodes atkarībā no klientūras vēlmēm un komunikācijas stratēģijas.

- tīmekļa vietne
- e-pasts
- ziņojumi
- arhivēšana un izpēte

CSIRT izplatītos konsultatīvos materiālus vajadzētu strukturēt vienādi. Tas atvieglos to lasāmību, un lasītājs varēs ātri atrast svarīgo informāciju.

Konsultatīvajā materiālā jāietver vismaz šāda informācija:

Konsultatīvā materiāla nosaukums ……
Atsauce Nr. …… **Skartās sitēmas** **-** …… **-** …… **Saistītā OS + versija** …… **Risks** (augsts-vidējs-zems) …… **Ietekme, iespējamie zaudējumi** (augsti-vidēji-zemi) …… **Ārējā id.:** (CVE, ievainojamības biļetena ID) ……
Pārskats par ievainojamību …… **Ietekme** …… **Risinājums** …… **Apraksts (detaļas)** …… **Pielikums** ……

12. att. Konsultatīvā materiāla shematisks piemērs

Pilnu konsultatīvā materiāla paraugu skatīt 10. nodaļā *Vingrinājums.*

8.3. Darbs ar incidentiem

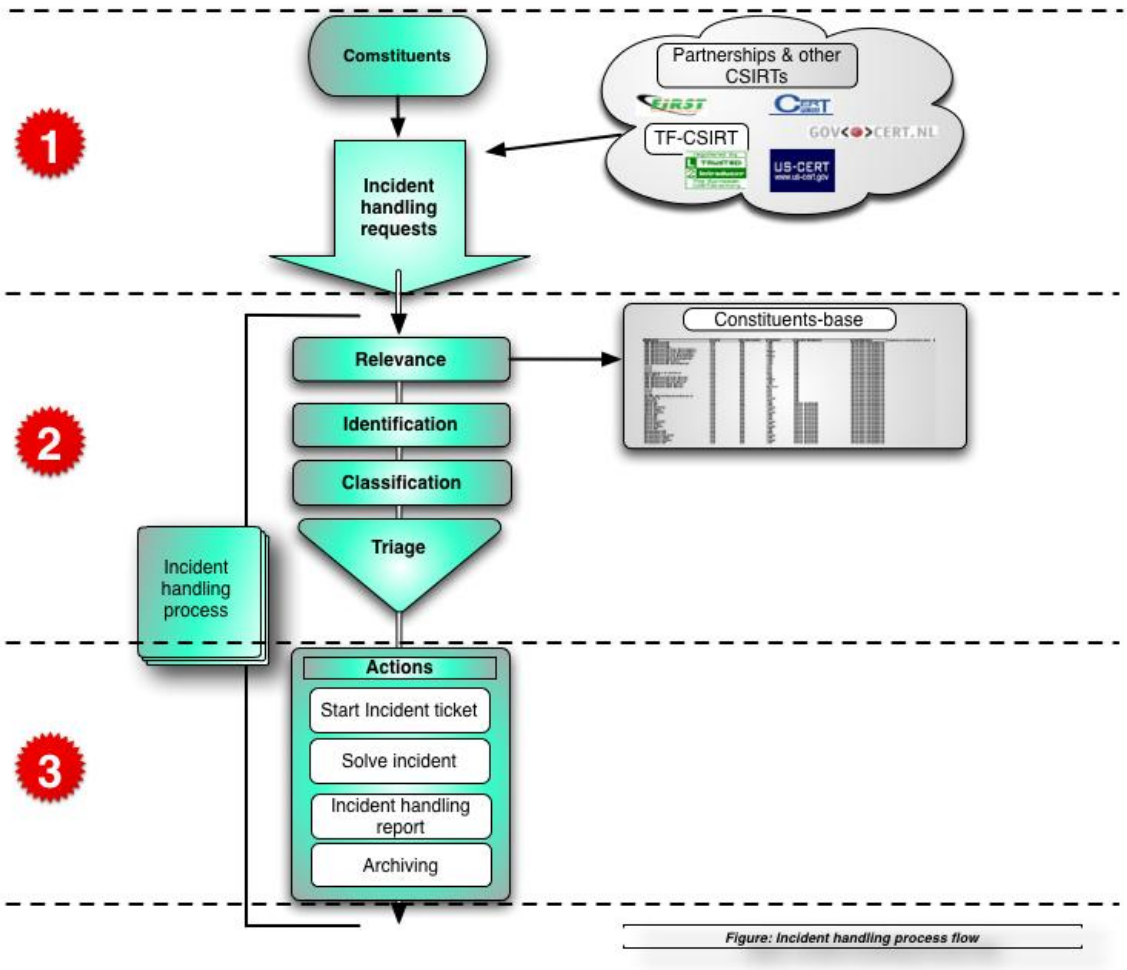
Kā minēts nodaļas ievadā, informācijas apstrādes process, strādājot ar incidentu, ļoti līdzinās trauksmes ziņojumu, brīdinājumu un paziņojumu veidošanas procesam. Taču informācijas ievākšanas darbs atšķiras, jo parasti datus par incidentu iegūst vai nu saņemot incidentu ziņojumus no klientūras vai citām vienībām, vai saņemot atbildes informāciju no citām iesaistītajām pusēm incidenta procesa laikā. Informācijas plūsma parasti notiek ar (kodēta) e-pasta starpniecību, dažreiz ir nepieciešams izmantot arī telefonu vai faksu.

Saņemot informāciju pa telefonu, vajadzētu atzīmēt pat vissīkākās detaļas, izmantojot kādu incidenta ziņojuma rīku vai izveidojot atgādni. Vajag nekavējoties (pirms sarunas noslēguma) piešķirt incidenta numuru (ja tas vēl nav izdarīts) un nodot to ziņotājam pa telefonu (vai ar vēlāk izsūtītu kopsavilkuma e-pastu). Numuru izmanto tālākajā komunikācijā kā atsauci.

Nodaļas pārējā daļā ir aprakstīts pamatprocess darbam ar incidentiem. Padziļinātu analīzi par visu incidentu vadības procesu un ar to saistītajām darbplūsmām un apakšplūsmām var atrast CERT/CC dokumentā *Incidentu pārvaldības procesu noteikšana CSIRT vajadzībām* [24].

[24] Incidentu pārvaldības procesu noteikšana: http://www.cert.org/archive/pdf/04tr015.pdf

Būtībā, strādājot ar incidentiem, darbplūsma ir šāda:



13. att. Incidentu analīzes process

1. uzdevums — seņemt ziņojumus par incidentiem

Kā minēts iepriekš, ziņojumi par incidentiem nokļūst CSIRT pa dažādiem kanāliem, galvenokārt pa e-pastu, bet arī pa telefonu un faksu.

Turklāt jau ir minēts, ka, saņemot ziņojumu par incidentu, visu informāciju vajadzētu pierakstīt noteiktā formātā. Tādā veidā tiek nodrošināts, lai netiek izlaista svarīga informācija. Veidlapas paraugs:

INCIDENTA ZIŅOJUMA VEIDLAPA
Lūdzu, aizpildiet šo veidlapu un nosūtiet to pa e-pastu vai faksu: …….. *Ar * atzīmētās ailes jāaizpilda obligāti.* *Personas vārds un organizācija* 1. Vārds*: 2. Organizācijas nosaukums*: 3. Sektors: 4. Valsts*: 5. Pilsēta: 6. E-pasta adrese*: 7. Telefons*: 8. Citas ziņas: *Skartais saimniekdators* 9. Saimnieku skaits: 10. Saimniekdatora nosaukums un IP*: 11. Saimniekfunkcija*: 12. Laika zona: 13. Aparatūra: 14. Operētājsistēma: 15. Skartā programmatūra: 16. Skartie faili: 17. Drošība: 18. Saimniekdatora nosaukums un IP: 19. Protokols, ports: *Incidents* 20. Atsauces Nr.: 21. Incidenta veids: 22. Incidenta sākums: 23. Tas ir ilgstošs incidents: JĀ NĒ 24. Atklāšanas laiks un metode: 25. Zināmās ievainojamības: 26. Aizdomīgie faili: 27. Pretpasākumi: 28. Sīks apraksts*:

14. att. Ziņojuma par incidentu saturs

2. uzdevums — incidenta novērtēšana

Šā uzdevuma mērķis ir pārbaudīt paziņotā incidenta autentiskumu un būtiskumu; incidents tiek klasificēts.

Identificēšana

Lai izvairītos no nevajadzīgām darbībām, vajadzētu pārbaudīt, vai ziņotājam var uzticēties un vai tas ir viens no jūsu vai kolēģu CSIRT klientūras pārstāvjiem. Tiek piemēroti noteikumi, kas līdzīgi 8.2. nodaļā „Trauksmes ziņojumu sastādīšana" aprakstītajiem.

Būtiskums

Šā uzdevuma mērķis ir pārbaudīt, vai lūgumu sākt darbu ar incidentu ir izteikusi CSIRT vienības klientūra un vai paziņotais incidents ir saistīts ar klientūras IT sistēmu. Ja tas nav ne viens, ne otrs gadījums, ziņojumu parasti nodot citai atbilstošai CISRT[25].

Klasifikācija

Klasificējot incidenta nopietnību, šajā solī tiek noteikta rīcības prioritāte. Detalizēta incidentu klasifikācija pārsniedz šī dokumenta ietvarus. Sākumam var izmantot CSIRT gadījumu klasifikācijas shēmu (uzņēmuma CSIRT piemērs):

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.		

15. att. Incidentu klasifikācijas shēma (avots: FIRST[26])

[25] Identitātes pārbaudes rīki CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] CSIRT gadījumu klasifikācija: http://www.first.org/resources/guides/csirt_case_classification.html

Prioritāšu noteikšana
Prioritāšu noteikšanas sistēmu izmanto medicīnas vai ārkārtas situāciju speciālisti, lai normētu ierobežotus medicīniskos resursus un aprūpētu iespējami lielāku pacientu skaitu apstākļos, kad ievainoto skaits, kam nepieciešama aprūpe, pārsniedz pieejamos resursus[27].

CERT/CC to raksturo šādi:

Prioritāšu noteikšana ir būtisks incidentu pārvaldības spējas elements, īpaši, ja CSIRT izveidojusies par stabilu vienību. Prioritāšu noteikšana ir kritisks elements izpratnē par to, kādi ziņojumi tiek saņemti visas organizācijas ietvaros. Tā kalpo kā instruments, ar kura palīdzību visa informācijas plūsma tiek novadīta uz vienu kontaktpunktu, dodot uzņēmumam iespēju vērtēt notiekošo darbību un iegūt visaptverošu priekšstatu par ziņotu datu saistību. Prioritāšu vērtēšana ļauj veikt ienākošā ziņojuma sākotnējo vērtējumu un noteikt tā kārtu tālākajā rīcībā. Turklāt tā sniedz iespēju sākt ziņojuma vai pieprasījuma dokumentēšanu un datu ievadi, ja tas jau nav paveikts atklāšanas procesā.

Prioritāšu vērtēšanas funkcija sniedz tūlītēju momentuzņēmumu par visu darbību pašreizējo statusu — kuri ziņojumi nav vai ir izskatīti, kāda rīcība ir veicama un cik katra veida ziņojumi ir saņemti. Šis process var palīdzēt noskaidrot iespējamās drošības problēmas un noteikt darba slodzes prioritāro sadalījumu. Prioritāšu noteikšanas laikā savākto informāciju var izmantot, lai noteiktu ievainojamību un incidentu tendences un sagatavotu statistiku augstākai vadībai[28].

Prioritāšu noteikšanu vajadzētu uzticēt tikai pašiem pieredzējušākajiem vienības locekļiem, jo ir nepieciešama dziļa izpratne par incidenta iespējamo ietekmi uz konkrētām klientūras grupām un spēja izlemt, kuram vienības loceklim vislabāk uzticēt darbu ar šo incidentu.

[27] „Prioritāšu noteikšana" Vikipēdijā: http://en.wikipedia.org/wiki/Triage

[28] Incidentu pārvaldības procesu noteikšana: http://www.cert.org/archive/pdf/04tr015.pdf

3. uzdevums — rīcība

Parasti incidenti ar noteikto prioritāti tiek ievietoti pieprasījumu rindā, izmantojot incidentu apstrādes rīku, ko lieto viens vai vairāki ar incidenta novēršanu saistītie darbinieki, kas būtībā veic šādas darbības:

Incidenta talona izrakstīšana
Iespējams, ka incidenta talona numurs jau ir piešķirts, pildot iepriekšējo uzdevumu (piemēram, kad par incidentu paziņoja pa telefonu). Ja nē, pirmais uzdevums ir piešķirt numuru, ko izmantos visās turpmākajās komunikācijās saistībā ar šo incidentu.

Incidenta dzīves cikls
Darbs ar incidentu nenotiek lineāru soļu veidā, kas noved pie risinājuma. Tās drīzāk ir lokveida darbības, kas tiek atkārtotas vairākas reizes, līdz visbeidzot incidents tiek atrisināts un visas iesaistītās puses iegūst vajadzīgo informāciju. Šis loks, ko bieži sauc par incidenta dzīves ciklu, ietver šādus procesus:

Analīze:	tiek analizēta visa informācija par paziņoto incidentu.
Kontaktinformācijas iegūšana:	lai varētu nodot ar incidentu saistīto informāciju visām iesaistītajām pusēm, piemēram, citām CSIRT vienībām, cietušajiem un, iespējams, sistēmu īpašniekiem, kurus pakļāva uzbrukumam.
Tehniskās palīdzības sniegšana:	palīdzība cietušajiem, lai tie varētu ātri likvidēt incidenta sekas, un papildu informācijas ievākšana par incidentu.
Koordinēšana:	citu iesaistīto pušu informēšana — piemēram, CSIRT vienības, kas atbildīga par uzbrukumā izmantoto IT sistēmu, vai citu cietušo informēšana.

Šo struktūru sauc par dzīves ciklu tāpēc, ka viens solis noved pie nākamā un pēdējais solis, koordinācija, var atkal novest pie jaunas analīzes, un cikls sākas no jauna. Process beidzas, kad visas iesaistītās puses ir saņēmušas un paziņojušas visu nepieciešamo informāciju.

Sīkāku aprakstu par incidenta dzīves ciklu skatīt CERT/CC CSIRT rokasgrāmatā[29].

Ziņojums par darbu ar incidentu
Sagatavojieties atbildēt uz vadības jautājumiem par incidentiem, sastādot ziņojumu. Būtu noderīgi uzrakstīt dokumentu (tikai lietošanai uzņēmuma iekšienē) par „gūtajām mācībām", lai izglītotu darbiniekus un izvairītos no kļūdām, turpmāk strādājot ar incidentiem.

[29] CSIRT rokasgrāmata: http://www.cert.org/archive/pdf/csirt-handbook.pdf

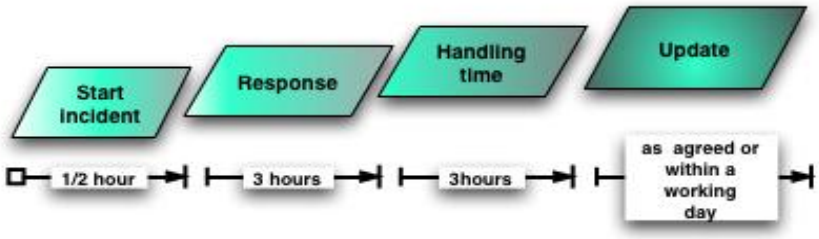
Arhivēšana
Skatiet arhivēšanas noteikumus, kas aprakstīti 6.6. nodaļā *Informācijas drošības politikas formulēšana.*

Informāciju par visaptverošām rokasgrāmatām par incidentu pārvaldību un incidentu dzīves ciklu skatiet pielikuma A.1. sadaļā *Cita literatūra*

8.4. Reaģēšanas grafika piemērs

Reaģēšanas laika noteikšana bieži tiek piemirsta, bet šim laikam jābūt iekļautam ikvienā labi sastādītā servisa līmeņa līgumā (SLA), kas noslēgts starp CSIRT un tās klientūru. CSIRT vienības spēja savlaicīgi reaģēt uz klientūras pieprasījumu ir ļoti svarīga gan saistībā ar klienta paša atbildības apjomu, gan vienības reputāciju.
Klientūra ir skaidri jāinformē par reaģēšanas laiku, lai izvairītos no nepamatotām cerībām. Šādu ļoti vienkāršu laika grafiku var izmantot kā sākumpunktu sīkāk izstrādātam servisa līmeņa līgumam, kas noslēgts ar klientūru.

Praktisks reaģēšanas laika grafiks, sniedzot palīdzību pēc pieprasījuma saņemšanas:



16. att. Piemērs — reaģēšanas laika grafiks

Klientūru vajadzētu arī informēt par viņu pašu reaģēšanas laiku, īpaši par to, kad sazināties ar CSIRT ārkārtas gadījumā. Vairumā gadījumu labāk ir sazināties ar CSIRT pēc iespējas agrāk, un vajadzētu mudināt, lai klientūra to darītu arī šaubu gadījumā.

8.5. Pieejamie CSIRT rīki

Šajā nodaļā sniegtas dažas norādes par parasti sastopamajiem rīkiem, ko izmanto CSIRT vienības. Tiek sniegti tikai piemēri, plašāka informācija atrodama izdevumā *Clearinghouse of Incident Handling Tools (Incidentu reaģēšanas rīku informācijas centrs)*[30] (CHIHT).

E-pasta un ziņojumu kodēšanas programmatūra

- GNUPG http://www.gnupg.org/
  GnuPG pilnībā realizēja GNU projekts, ieviešot bezmaksas OpenPGP standartu saskaņā ar RFC2440. GnupPG sniedz iespēju kodēt un parakstīt datus un ziņojumus.

- Šifrēšanas tehnika PGP http://www.pgp.com/
  Komerciālais variants

Rīks darbam ar incidentiem

Administrē un novēro incidentus, sekojot veiktajām darbībām.

- RTIR http://www.bestpractical.com/rtir/
  RTIR ir atklāta pirmkoda bezmaksas sistēma darbam ar incidentiem, kas izveidota CERT un citu incidentu reaģēšanas vienību vajadzībām.

CRM rīki

Kad ir daudz klientu un ir nepieciešams izsekot visiem norīkojumiem un informācijai, noder CRM. Ir daudz dažādu variantu. Daži piemēri:

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

- Sugarforce (bezmaksas atklāta pirmkoda versija)
  http://www.sugarforge.org/

Informācijas pārbaude

- tīmekļa vietņu pārraugs
  http://www.aignes.com/index.htm
  Šī programma pārrauga tīmekļa vietņu atjaunināšanu un izmaiņas.

- Watch that page (vēro to lapu)
  http://www.watchthatpage.com/
  Pakalpojuma ietvaros pa e-pastu (bez maksas vai komerciāli) tiek nosūtīta informācija par izmaiņām tīmekļa vietnēs.

Kontaktinformācijas meklēšana

Atrast pareizo kontaktpersonu incidentu paziņošanai nav vienkāršs uzdevums. Pāris informācijas avoti, ko var izmantot:

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

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

Turklāt CHIHT piedāvā rīku sarakstu kontaktinformācijas meklēšanai[34].

Fiktīvā CSIRT (8. uzdevums)

Procesu norises, operatīvo un tehnisko procedūru noteikšana

Fiktīvā CSIRT pievērš uzmanību CSIRT pamatpakalpojumu sniegšanai:

- trauksmes ziņojumi un brīdinājumi,
- paziņojumi,
- darbs ar incidentiem.

Vienība izstrādā procedūras, kas labi funkcionē un ir viegli saprotamas visiem vienības locekļiem. Fiktīvā CSIRT pieņem darbā arī juristu, kas nodarbojas ar tiesiskās atbildības jautājumiem un informācijas drošības politiku. Apspriežoties ar citām CSIRT vienībām, jaunā vienība apgūst lietderīgus rīkus un iegūst noderīgu informāciju par operatīviem jautājumiem.

Tiek izveidota noteikta veidne konsultatīvo drošības materiālu un incidentu ziņojumu sastādīšanai. Darbam ar incidentiem vienība izmanto RTIR.

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

[32] IRT-object RIPE datu bāzē: 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] Identitātes pārbaudes rīki CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9. CSIRT apmācība

Līdz šim izpildīti šādi uzdevumi:

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.
2. Kādam sektoram tiks sniegti jaunās CSIRT vienības pakalpojumi?
3. Kāda veida pakalpojumus CSIRT var sniegt savai klientūrai.
4. Klientūras un vides analīze.
5. Misijas formulēšana.
6. Biznesa plāna sastādīšana.
   a. Finanšu modeļa definēšana.
   b. Organizācijas struktūras noteikšana.
   c. Darbinieku pieņemšana.
   d. Biroja telpas un iekārtas.
   e. Informācijas drošības politikas formulēšana.
   f. Sadarbības partneru meklēšana.
7. Biznesa plāna virzīšana.
   a. Darbības pamatojuma apstiprināšanas panākšana.
   b. Visu punktu apkopošana projekta plānā.
8. CSIRT darbības uzsākšana.
   a. Darbplūsmu sastādīšana.
   b. CSIRT rīku ieviešana.

>> Nākamais uzdevums — darbinieku apmācība.

Šajā nodaļā minēti divi galvenie specializētās CSIRT apmācības avoti: TRANSITS un CERT/CC kursi.

9.1. TRANSITS

TRANSITS ir Eiropas projekts, kura mērķis ir veicināt datoru drošības incidentu reaģēšanas vienību (CSIRT) izveidi un sekmēt esošo CSIRT vienību darbu, risinot problēmu, kas pastāv attiecībā uz kvalificētu CSIRT darbinieku trūkumu. Šajā nolūkā (jaunu) CSIRT vienību darbiniekiem tiek sniegti specializēti apmācības kursi par organizatoriskiem, operatīviem, tehniskiem, tirgus un juridiskiem jautājumiem, kas saistīti ar CSIRT pakalpojumu sniegšanu.

TRANSITS:

- izstrādā, atjauno un regulāri pārskata modulāro apmācības kursu materiālus;
- organizē apmācību darbseminārus, kuros tiek sniegti kursu materiāli;
- sniedz iespēju (jaunu) CSIRT vienību darbiniekiem piedalīties apmācības darbseminārōs, īpaši piesaistot ES pievienošanās valstu pārstāvjus;
- izplata apmācības kursu materiālus un nodrošina apgūtā materiāla pielietošanu[35].

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

ENISA veicina un atbalsta TRANSITS kursus. Ja vēlaties uzzināt, kā pieteikties kursos, kādas ir prasības un izmaksas, lūdzu, sazinieties ar ENISA CSIRT speciālistiem:

CERT-Relations@enisa.europa.eu

Kursa materiālu paraugi atrodami šī dokumenta pielikumā.

9.2. CERT/CC

Nodrošināt pienācīgu tīklu drošību ir grūti, jo datoru un tīklu infrastruktūra un tās administrēšana ir sarežģīta. Tīklu un sistēmu administratoriem nav pietiekami daudz cilvēku un drošības procedūru, lai novērstu uzbrukumus un mazinātu zaudējumus. Tāpēc datoru drošības incidentu skaits pieaug.
Kad notiek datoru drošības incidents, organizācijai ir jāreaģē ātri un efektīvi. Jo ātrāk organizācija atpazīs, izanalizēs un reaģēs uz incidentu, jo mazāki būs tās zaudējumi un seku likvidēšanas izmaksas. Datoru drošības incidentu reaģēšanas vienības (CSIRT) izveide ir labs veids, kā nodrošināt spēju ātri reaģēt un novērst incidentus nākotnē.

CERT-CC piedāvā kursus vadītājiem un tehniskajiem darbiniekiem tādās jomās kā datoru drošības incidentu reaģēšanas vienību (CSIRT) izveide un vadīšana, reaģēšana uz drošības incidentiem un to analīze, tīklu drošības uzlabošana. Ja nav norādīts citādi, visi kursi notiek Pitsburgā, PA. Mūsu štata darbinieki pasniedz kursus par drošības jautājumiem arī Karnegi Mellona Universitātē.

CERT/CC kursi[36] , kas paredzēti CSIRT vienībām

Datoru drošības incidentu reaģēšanas vienības izveide (CSIRT)
Datoru drošības incidentu reaģēšanas vienību (CSIRT) vadīšana
Darba ar incidentiem pamatprincipi
Padziļināts kurss tehniskajiem darbiniekiem, kas strādā ar incidentiem

Kursu materiālu paraugi atrodami šī dokumenta pielikumā.

Fiktīvā CSIRT (9. uzdevums)
Darbinieku apmācība Fiktīvā CSIRT pieņem lēmumu par darbinieku nosūtīšanu uz nākamajiem TRANSITS kursiem. Turklāt vienības vadītājs apmeklē CERT/CC kursu par CSIRT vadīšanu.

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

10. Vingrinājums — konsultatīvā materiāla izveide

Līdz šim izpildīti šādi uzdevumi:

1. Gūta izpratne par to, kas ir CSIRT un kādas priekšrocības tā sniedz.
2. Kādam sektoram tiks sniegti jaunās CSIRT vienības pakalpojumi?
3. Kāda veida pakalpojumus CSIRT var sniegt savai klientūrai.
4. Klientūras un vides analīze.
5. Misijas formulēšana.
6. Biznesa plāna sastādīšana.
   a. Finanšu modeļa definēšana.
   b. Organizācijas struktūras noteikšana.
   c. Darbinieku pieņemšana.
   d. Biroja telpas un iekārtas.
   e. Informācijas drošības politikas formulēšana.
   f. Sadarbības partneru meklēšana.
7. Biznesa plāna virzīšana.
   a. Darbības pamatojuma apstiprināšanas panākšana.
   b. Visu punktu apkopošana projekta plānā.
8. CSIRT darbības sākšana.
   a. Darbplūsmu sastādīšana
   b. CSIRT rīku ieviešana.
9. Darbinieku apmācība.

>> Nākamais uzdevums ir izpildīt vingrinājumus un sagatavoties reālajam darbam!

Šajā nodaļā CSIRT ikdienas uzdevuma paraugs, konsultatīvā materiāla sastādīšana, ir dots kā piemērs.

To rosināja šāds Microsoft izsūtīts konsultatīvais drošības materiāls:

Biļetena identifikators	**Microsoft drošības biļetens MS06-042**
Biļetena nosaukums	**Kopējais Internet Explorer drošības atjauninājums (918899)**
Kopsavilkums	Šis atjauninājums atrisina vairākas Internet Explorer ievainojamības, kas pieļāva koda attālo izpildi.
Maksimālais nopietnības novērtējums	SKritisks
Ievainojamības ietekme	Koda attālā izpilde
Skartā programmatūra	**Windows, Internet Explorer.** Plašāku informāciju skatīt sadaļā Skartā programmatūra un Lejupielādēt vietas.

Šajā pārdošanas organizācijām paredzētajā biļetenā apskatīta nesen atklāta *Internet Explorer* ievainojamība. Pārdevējs publicē vairākus programmatūras labošanas veidus dažādām *Microsoft Windows* versijām.

Pa e-pastu saņemot informāciju par ievainojamību, fiktīvā CSIRT realizē procedūru, kas aprakstīta 8.2. nodaļā „Trauksmes ziņojumu, brīdinājumu un paziņojumu sastādīšana”.

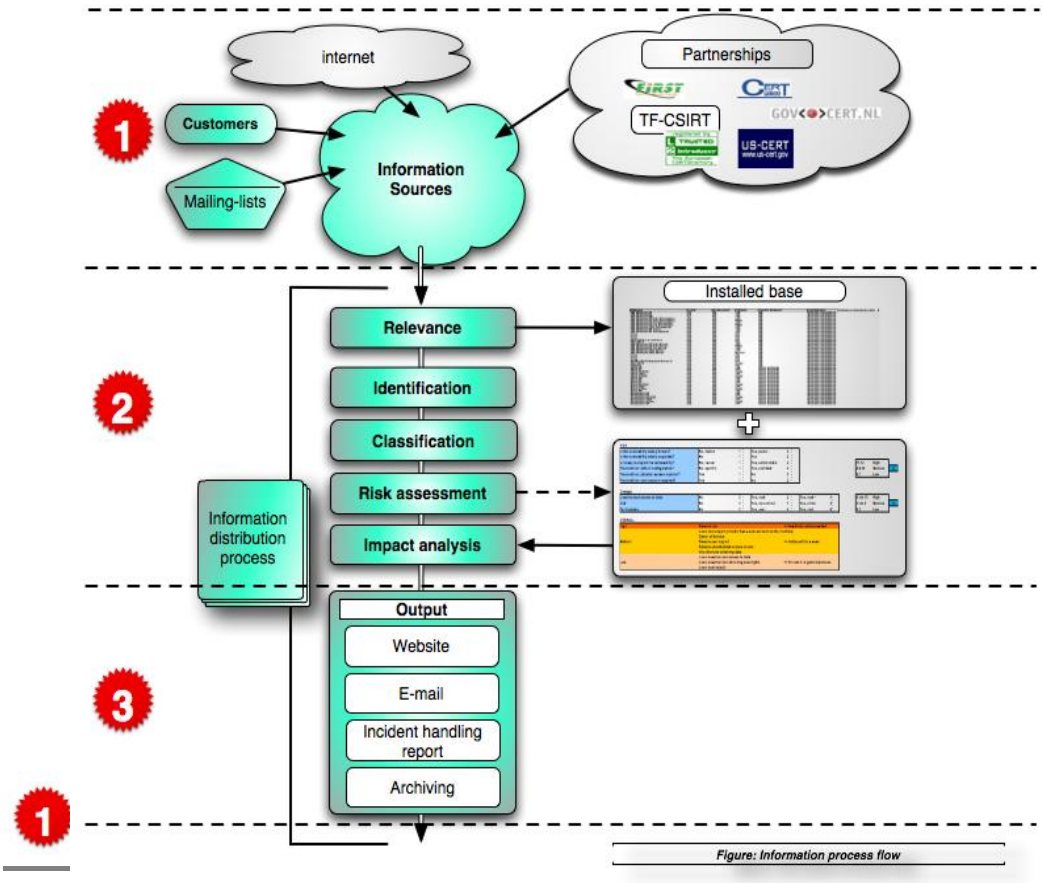


Figure: Information process flow

1. uzdevums — informācijas ievākšana par ievainojamību.

Pirmais solis ir doties uz pārdevēja tīmekļa vietni. Fiktīvā CSIRT pārliecinās par informācijas autentiskumu un ievāc papildu datus par ievainojamību un IT sistēmām.

2. uzdevums — informācijas un riska novērtēšana

Identificēšana
Informācija jau ir pārbaudīta, salīdzinot pa e-pastu saņemto informāciju par ievainojamību ar tekstu pārdevēja tīmekļa vietnē.

Būtiskums
Fiktīvā CSIRT pārbauda skarto sistēmu sarakstu, kas atrodams tīmekļa vietnē, ar klientūras lietoto sistēmu sarakstu. Tiek noskaidrots, ka vismaz viens klientūras pārstāvis lieto *Internet Explorer*, un tāpēc informācija pa ievainojamību ir būtiska.

Kategorija	Pielietojums	Programmatūras produkts	Versija	OS	OS versija	Klientūra
darbvirsma	pārlūks	IE	x-x-	Microsoft	XP-prof	A

Klasifikācija
Informācija ir publiska, un tāpēc to var izmantot un izplatīt.

Riska novērtējums un ietekmes analīze
Atbildot uz jautājumiem, redzams, ka risks un tā ietekme ir *liela* (Microsoft to novērtējis kā kritisku).

RISKS

Vai ievainojamība ir zināma?	Jā
Vai ievainojamība ir izplatīta?	Jā
Vai ievainojamību var viegli izmantot?	Jā
Vai ievainojamību var izmantot, iedarbojoties attāli?	Jā

ZAUDĒJUMI
Iespējamā ietekme ir attālā piekļuve un, iespējams, attāla koda izpilde. Šī ievainojamība ietver daudzas problēmas, kas zaudējuma riskam piešķir *augstu* pakāpi.

3. uzdevums — izplatīšana

Izdomātā CSIRT ir uzņēmuma iekšējā CSIRT. Tai ir e-pasts, telefons un iekšēja tīmekļa vietne, ko var izmantot kā komunikācijas kanālus. CSIRT izveido konsultatīvo materiālu, izmantojot veidni, kas minēta 8.2. nodaļā *Trauksmes ziņojumu, brīdinājumu un paziņojumu sastādīšana.*

Konsultatīvā materiāla nosaukums
Internet Explorer konstatētas daudzas ievainojamības

Atsauce Nr.
082006-1
Skartās sistēmas
- Visas galddatoru sistēmas, kas izmanto Microsoft

Saistītā OS + versija
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 un Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 un Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 Itanium sistēmām un Microsoft Windows Server 2003 ar SP1 Itanium sistēmām
- Microsoft Windows Server 2003 x64 versija

Risks (augsts-vidējs-zems)
AUGSTS
Ietekme, iespējamie zaudējumi (augsti-vidēji-zemi)
AUGSTI
Ārējā id: (CVE, ievainojamības biļetena ID)
MS-06-42

Pārskats par ievainojamību
Microsoft ir konstatējis vairākas kritiskas Internet Explorer ievainojamības, kas pieļauj koda attālo izpildi.

Ietekme
Uzbrucējs var pārņemt visu sistēmu, instalējot programmas, pievienojot lietotājus, un mainīt un dzēst datus. Risku mazina tas, ka iepriekš minētais var notikt tikai, ja lietotājs ir pieteicies ar administratora tiesībām. Pieteikušos lietotājus, kas neizmanto administratora tiesības, var ietekmēt mazāk.

Risinājums
Nekavējoties pielabot IE.

Apraksts (detaļas)
Vairāk informācijas skatīt ms06-042.mspx

Pielikums
Vairāk informācijas skatīt ms06-042.mspx

Izveidotais materiāls ir gatavs izplatīšanai. Tā kā šis ir ļoti svarīgs biļetens, klientūras pārstāvjiem ir ieteicams arī piezvanīt, kad iespējams.

Fiktīvā CSIRT (10. uzdevums)
Vingrinājumi Darbības pirmajā nedēļā fiktīvā CSIRT vingrinājumiem izmanto vairākus fiktīvus gadījumus (tos viņi piemēru veidā saņēma no citām CSIRT vienībām). Turklāt viņi izdod dažus konsultatīvos drošības materiālus, balstoties uz aparatūras un programmatūras pārdevēju izplatīto informāciju par īstām ievainojamībām, ko viņi pielāgo savas klientūras vajadzībām.

11. Nobeigums

Līdz ar to rokasgrāmata ir galā. Šī dokumenta nolūks bija sniegt ļoti kodolīgu pārskatu par dažādiem procesiem, kas veicami, lai izveidotu CSIRT. Dokuments nepretendē uz pilnīgumu, un tas pārāk neiedziļinās specifiskās detaļās. Lai atrastu noderīgu literatūru par šo tēmu, skatiet pielikuma A.1. sadaļu *Cita literatūra.*

Nākamie svarīgie uzdevumi, kas veicami fiktīvajai CSIRT, būtu šādi:

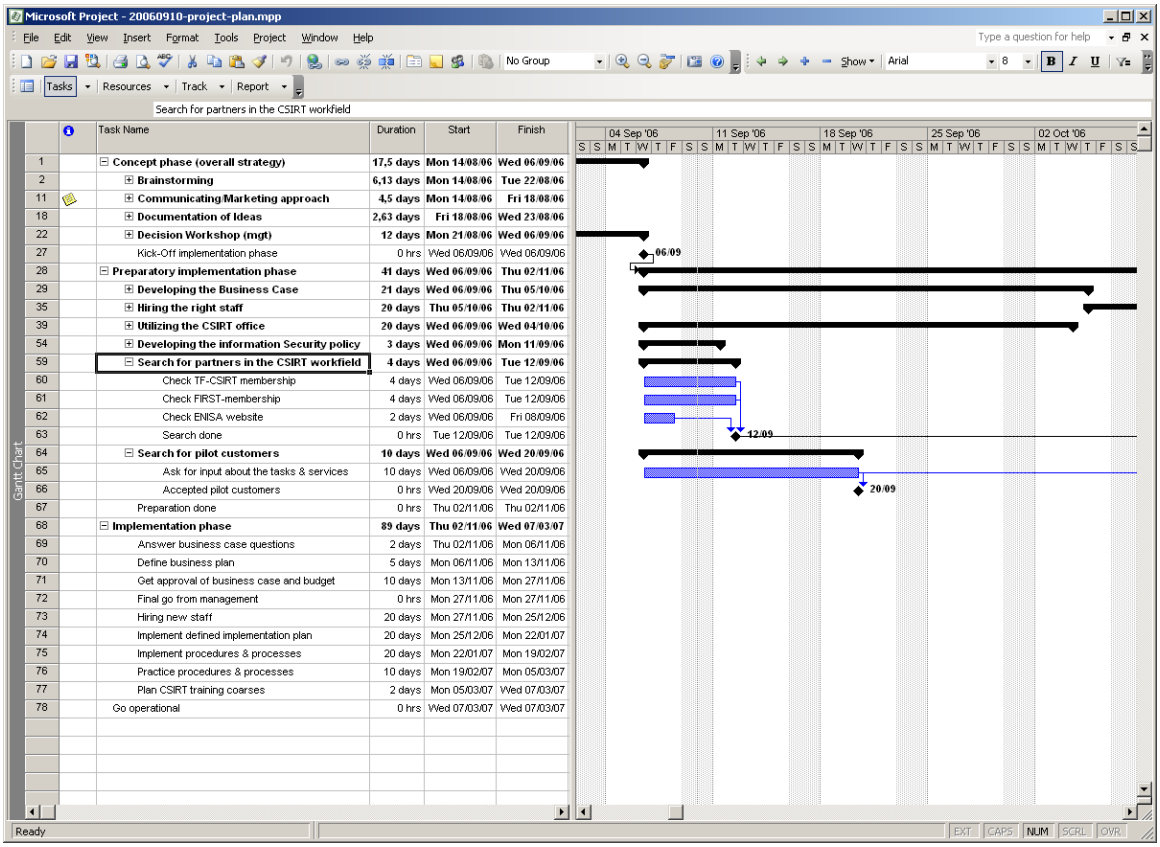
- saņemt atsauksmes no klientūras, lai uzlabotu sniegtos pakalpojumus;
- panākt procedūru izpildi ikdienas darbā;
- vingrināties ārkārtas situācijām;
- uzturēt ciešu saikni ar dažādām CSIRT kopienām ar mērķi kādu dienu dot savu ieguldījumu viņu brīvprātīgajā darbā.

12. Projekta plāna apraksts

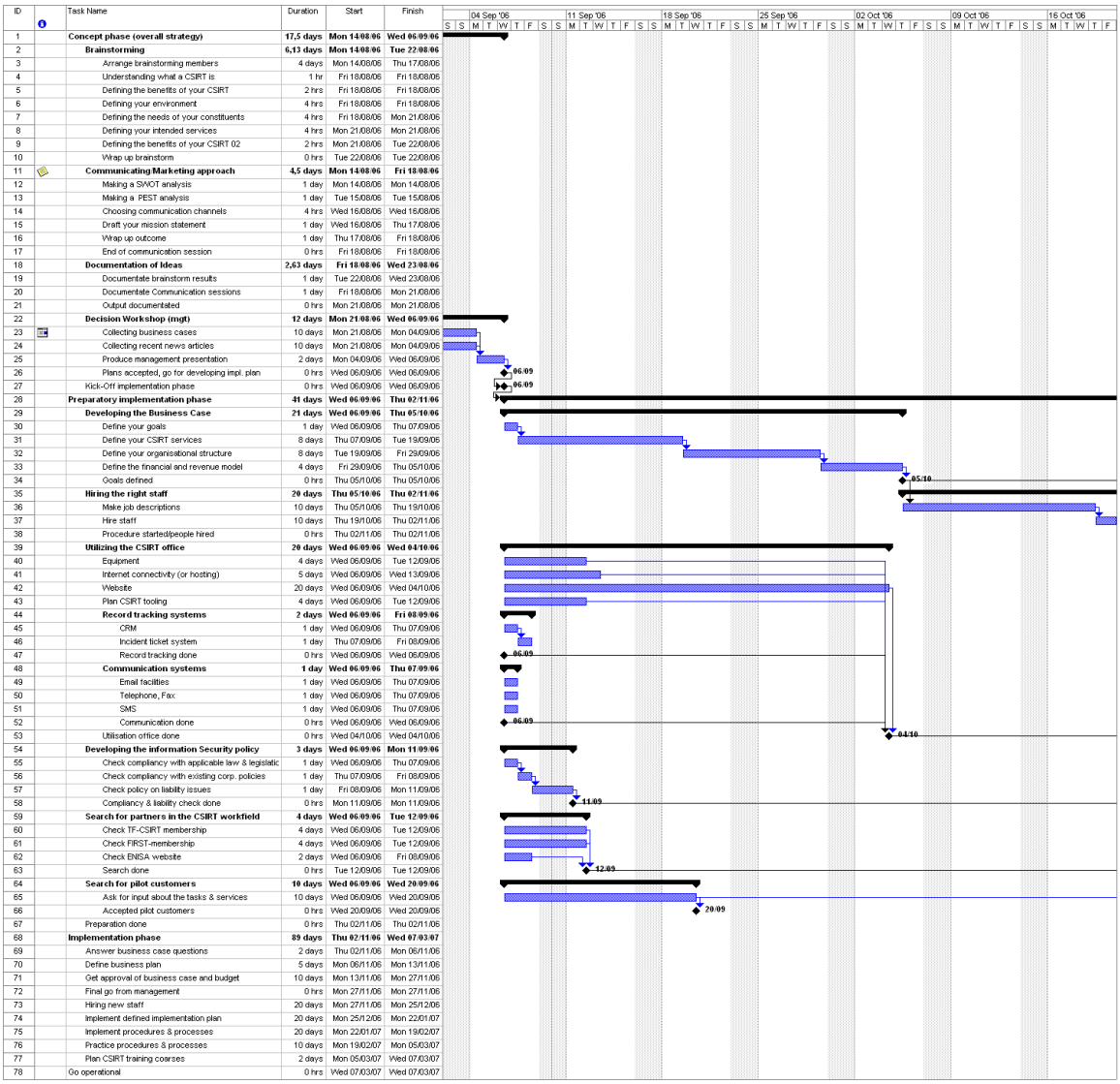
PIEZĪME. Projekta plāns sniedz pirmo aplēsi par projektam vajadzīgo laiku. Atkarībā no resursu pieejamības īstais projekta ilgums var atšķirties.

Projekta plāns ir pieejams dažādos formātos uz kompaktdiska un ENISA tīmekļa vietnē. Tas pilnībā aptver visus šai dokumentā aprakstītos procesus.

Galvenais ir Microsoft Project formāts, tāpēc to var tieši izmantot šī projekta pārvaldības rīkā.



17. att. Projekta plāns



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

18. att. Projekta plāns ar visiem uzdevumiem un daļu no Ganta grafika.

Projekta plāns ir pieejams arī CVS un XML formātā. Citus izmantošanas veidus var pieprasīt no ENISA CSIRT speciālistiem: CERT-Relations@enisa.europa.eu

PIELIKUMS

A.1. Cita literatūra

Handbook for CSIRTs (Rokasgrāmata CSIRT vienībām)
Visaptverošs uzziņu materiāls par visiem jautājumiem, kas saistīti ar CSIRT darbu.
Avots: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress (Incidentu pārvaldības procesu noteikšana CSIRT vienību vajadzībām — darbs procesā)
Padziļināta incidentu pārvaldības analīze.
Avots: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs) (Datoru drošības incidentu reaģēšanas vienību (CSIRT) pašreizēja prakse)
Visaptveroša analīze par faktisko situāciju CSIRT jomā visā pasaulē, ieskaitot vēsturi, statistiku un daudz ko citu.
Avots: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box (CERT komplekts)
Visaptverošs apraksts par pieredzi, kas gūta, izveidojot GOVCERT.NL un 'De Waarschuwingsdienst' — Holandes valsts trauksmes ziņojumu dienestu.
Avots: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response (Kas tiek sagaidīts no datoru drošības incidentu reaģēšanas)
Avots: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide (Rokasgrāmata darbam ar datoru drošības incidentiem)
Avots: http://www.securityunit.com/publications/sp800-61.pdf

ENISA Inventory of CERT activities in Europe (Enisa uzskaite par CERT aktivitātēm Eiropā)
Uzziņu materiāls, kurā apkopota visa informācija par CSIRT vienībām Eiropā un to dažādajām aktivitātēm.
Avots: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: National Institute of Standards and Technologies (Standartu un tehnoloģiju valsts institūts)

A.2. CSIRT pakalpojumi

Īpaša pateicība pienākas CERT/CC, kas sniedza šo sarakstu.

Reaģēšanas pakalpojumi	***Proaktīvas rīcības pakalpojumi***	***Darinājumu apstrāde***
• Trauksmes un brīdinājumi • Darbs ar incidentiem • Incidentu analīze • Reaģēšana uz incidentiem objektā • Atbalsts, reaģējot uz incidentiem • Koordinācija, reaģējot uz incidentiem • Darbs ar ievainojamību • Ievainojamības analīze • Reaģēšana uz ievainojamību • Koordinācija, reaģējot uz ievainojamību	• Paziņojumi • Tehnoloģijas uzraudzīšana • Drošības auditi vai vērtējumi • Drošības konfigurēšana un uzturēšana • Drošības rīku izveide • Ielaušanās atklāšanas pakalpojumi • Ar drošību saistītas informācijas izplatīšana	• Darinājumu analīze • Reaģēšana uz darinājumiem • Koordinēšana, reaģējot uz darinājumiem ***Drošības kvalitātes vadība*** • Riska analīze • Darbības nepārtrauktība un seku likvidācija • Konsultācijas drošības jautājumos • Izpratnes veidošana • Izglītība, apmācība • Produktu novērtējums vai sertifikācija

19. att. CSIRT pakalpojumu saraksts no CERT/CC:

Pakalpojuma apraksts

Reaģēšanas pakalpojumi

Reaģēšanas pakalpojumi paredzēti, lai atbildētu uz CSIRT klientūras palīdzības lūgumiem, ziņojumiem par incidentiem un draudiem vai uzbrukumiem, kas vērsti pret CSIRT sistēmām. Atsevišķu pakalpojumu sniegšanu var iniciēt trešo pušu ziņojumi vai uzraugot IDS žurnālus un trauksmes ziņojumus.

Trauksmes ziņojumi un brīdinājumi

Šis pakalpojums saistīts ar tādas informācijas izplatīšanu, kas apraksta uzbrukumu, drošības ievainojamību, iebrukuma trauksmi, datorvīrusu vai ļaunu joku un iesaka īslaicīgus pasākumus radušos problēmu likvidēšanai. Trauksme, brīdinājums vai konsultatīvais materiāls tiek nosūtīts, reaģējot uz pašreizēju problēmu, lai informētu klientūras pārstāvjus par notikušo un sniegtu ieteikumus sistēmas aizsardzībai vai skarto sistēmu atjaunošanai. Informāciju var sastādīt pati CSIRT vienība vai arī tā var izplatīt no tirgotājiem, citām CSIRT vienībām, drošības speciālistiem vai citām klientūras vienībām saņemto informāciju.

Darbs ar incidentiem

Darbs ar incidentiem ietver lūgumu un ziņojumu pieņemšanu, to prioritātes noteikšanu un reaģēšanu uz tiem, kā arī incidentu un atgadījumu analīzi. Konkrēta reaģēšanas rīcība var ietvert:

- pasākumu veikšanu, lai aizsargātu sistēmas un tīklus, ko skārušas vai draud skart iebrucēju darbības,
- risinājumu un seku mazināšanas stratēģijas izstrādi, ņemot vērā attiecīgos konsultatīvos materiālus un trauksmes ziņojumus
- iebrucēju darbības pēdu meklēšanu citās tīkla daļās,
- tīkla datplūsmas filtrēšanu,
- sistēmu pārveidošanu,
- sistēmu pielabošanu vai labošanu,
- citu reaģēšanas stratēģiju un alternatīvu risinājumu meklēšanu.

Tā kā darbu ar incidentiem veic dažādas CSIRT vienības, izmantojot dažādas metodes, šo pakalpojumu dala sīkākās kategorijās pēc veiktās darbības un sniegtās palīdzības veida.

Incidentu analīze

Ir daudzi incidentu analīzes līmeņi un dažādi apakšpakalpojumi. Būtībā incidentu analīze ietver visas pieejamās informācijas un ar incidentu vai atgadījumu saistīto pierādījumu jeb materiālu izvērtēšanu. Analīzes mērķis ir noskaidrot incidenta un tā radīto bojājumu apmēru, incidenta raksturu un pieejamās reaģēšanas stratēģijas vai alternatīvos risinājumus. CSIRT var izmantot ievainojamības vai darinājumu analīzes (aprakstīta tālāk tekstā) rezultātus, lai izprastu un sniegtu vispilnīgāko un jaunāko analīzi par to, kas noticis konkrētajā sistēmā. CSIRT salīdzina darbības dažādos incidentos, lai noskaidrotu saistības, tendences, iezīmes vai iebrucēju rokrakstu. Divi apakšpakalpojumi, ko atkarībā no CSIRT misijas, mērķa un procesiem var sniegt kā daļu no incidentu analīzes, ir šādi.

Tiesas pierādījumu vākšana

No skartās datoru sistēmas iegūto pierādījumu vākšana, saglabāšana, dokumentēšana un analizēšana, lai noskaidrotu sistēmas izmaiņas un palīdzētu rekonstruēt notikumus, kas izraisīja bojājumu. Informācija un pierādījumi jāvāc tā, lai tiktu dokumentēta pierādāma fizisko pierādījumu kustība un piederība, kas ir akceptējama izskatīšanai tiesā saskaņā ar pierādījumu noteikumiem. Tiesu izmeklēšanas ietvaros veikto pierādījumu vākšana ietver (bet neaprobežojas) skartās sistēmas cietā diska bitu attēla kopijas izveidi, sistēmas izmaiņu pārbaudi (programmu, failu, sniegto pakalpojumu un lietotāju), notiekošo procesu un atvērto portu pārbaudi, un Trojas zirgu (programmu vai rīkkopu) meklēšanu. CSIRT darbiniekiem, kas veic šīs funkcijas, jābūt gataviem liecināt tiesā kā ekspertiem.

Izcelsmes noskaidrošana

Iebrucēja izcelsmes noskaidrošana vai tās sistēmas noteikšana, kurai iebrucējs varēja piekļūt. Veicot šīs darbības, tiek izsekots ceļš, pa kādu iebrucējs iekļuva skartajās sistēmās vai saistītajos tīklos, kādas sistēmas tika izmantotas piekļuvei, kur uzbrukums sākās un kādas citas sistēmas un tīkli tika izmantoti uzbrukuma realizēšanai. Uzbrucēja identitātes noskaidrošana arī var būt šī darba sastāvdaļa. Šo darbu var veikt autonomi,

bet parasti to veic sadarbībā ar tiesībsargājošām iestādēm, interneta pakalpojumu sniedzējiem vai citām iesaistītajām organizācijām.

Reaģēšana uz incidentiem objektā

CSIRT sniedz palīdzību tieši notikuma vietā, lai klientūras pārstāvjiem palīdzētu likvidēt incidenta sekas. CSIRT veic skarto sistēmu fizisko analīzi un veic sistēmu remontus un labošanu, nevis sniedz incidentu reaģēšanas atbalstu tikai pa telefonu vai e-pastu (skatīt tālāk tekstā). Šis pakalpojumus aptver visas vietējā līmenī veiktās darbības, kas nepieciešamas, ja ir aizdomas par incidentu vai ja tas noticis. Ja CSIRT neatrodas skartajā objektā, vienības locekļi dodas uz turieni un veic savu darbu. Citos gadījumos vietējā vienība jau var būt uz vietas, reaģējot uz incidentu sava ikdienas darba ietvaros. Tā parasti notiek, ja darbu ar incidentu veic nevis atsevišķa CSIRT vienība, bet gan sistēmas, tīkla vai drošības administrators savu parasto pienākumu ietvaros.

Atbalsts, reaģējot uz incidentiem

CSIRT sniedz palīdzību un ieteikumus pa telefonu, e-pastu, faksu vai nodrošinot dokumentāciju, lai uzbrukumā cietušie varētu likvidēt incidenta sekas. Tā var būt tehniska palīdzība, interpretējot ievāktos datus, sniedzot kontaktinformāciju vai sniedzot norādījumus par seku mazināšanas un likvidēšanas stratēģiju. Tā nav saistīta ar tiešu reaģēšanas pasākumu veikšanu notikuma vietā, kā aprakstīts iepriekš. CSIRT sniedz padomus attāli tā, lai objekta darbinieki paši varētu likvidēt incidenta sekas.

Koordinēšana, reaģējot uz incidentiem

CSIRT koordinē reaģēšanas pasākumus, ko veic incidentā iesaistītās puses. Koordinācija parasti aptver uzbrukumā cietušo, citus uzbrukumā iesaistītos objektus un jebkurus citus objektus, kam nepieciešama palīdzība uzbrukuma analizēšanā. Tā var ietvert arī puses, kas cietušajam sniedz IT atbalstu, piemēram, interneta pakalpojumu sniedzējus, citas CSIRT vienības un sistēmas un tīkla administratorus objektā. Koordinācijas darbs var būt saistīts ar kontaktinformācijas ievākšanu, objektu brīdināšanu par to iespējamo saistību (kā cietušā vai uzbrukuma avota), statistikas apkopošanu par iesaistīto objektu skaitu un informācijas apmaiņas un analīzes atvieglošanu. Daļa no koordinācijas darba var būt saistīta ar organizācijas juriskonsulta, cilvēkresursu vai sabiedrisko attiecību nodaļas informēšanu un sadarbību ar tiem. Šis darbs ietver arī koordināciju ar tiesībsargājošām iestādēm. Šis pakalpojums nav saistīts ar tiešu reaģēšanas pasākumu veikšanu notikuma vietā.

Darbs ar ievainojamību

Darbs ar ievainojamību ietver informācijas un ziņojumu saņemšanu par aparatūras un programmatūras ievainojamībām; ievainojamību rakstura, mehānisma un efekta analizēšanu; reaģēšanas pasākumu stratēģijas izveidi, lai noskaidrotu un likvidētu ievainojamības. Tā kā darbu ar ievainojamībām veic dažādas CSIRT vienības, izmantojot dažādas metodes, šo pakalpojumu dala sīkākās kategorijās pēc veiktās darbības un sniegtās palīdzības veida.

Ievainojamības analīze

CSIRT veic aparatūras un programmatūras ievainojamību tehnisko analīzi un izvērtēšanu. Tas ietver iespējamo ievainojamību faktisko konstatāciju un aparatūras vai programmatūras ievainojamības tehnisko pārbaudi, lai noskaidrotu, kur tā atrodas un kā

to var izmantot. Šī analīze var ietvert pirmkoda pārbaudi, atkļūdotāja izmantošanu, lai noskaidrotu ievainojamības atrašanos, vai problēmas rekonstruēšanu testēšanas sistēmā.

Reaģēšana uz ievainojamību

Šī pakalpojuma ietvaros tiek noskaidrots, kādi reaģēšanas pasākumi ir piemēroti ievainojamības mazināšanai vai likvidēšanai. Tas var nozīmēt ielāpu, labojumu un alternatīvu risinājumu izstrādi vai izpēti. Tas ietver arī citu pušu informēšanu par seku mazināšanas stratēģiju, iespējams, izveidojot un izplatot konsultatīvos materiālus un trauksmes ziņojumus. Pakalpojums var ietvert reaģēšanas pasākumus — ielāpu, labojumu vai alternatīvo risinājumu instalēšanu.

Koordinēšana, reaģējot uz ievainojamību

CSIRT informē uzņēmuma vai klientūras vienības par ievainojamību un sniedz informāciju par to, kā novērst vai mazināt ievainojamību. CSIRT pārliecinās, ka stratēģija reaģēšanai uz ievainojamību ir sekmīgi īstenota. Šis pakalpojums var ietvert saziņu ar tirgotājiem, citām CSIRT vienībām, tehniskiem ekspertiem, klientūras pārstāvjiem, indivīdiem vai grupām, kas atklāja vai ziņoja par ievainojamību. Pasākumi ietver palīdzību ievainojamības vai ievainojamības ziņojuma analīzē, atbilstošo dokumentu publicēšanas, ielāpu vai alternatīvo risinājumu izlaišanas grafika koordināciju un dažādu pušu veikto tehnisko analīžu sintēzi. Pakalpojums var ietvert arī publiska vai privāta arhīva vai datu bāzes uzturēšanu, kas satur informāciju par ievainojamību un atbilstošām reaģēšanas stratēģijām.

Darbs ar darinājumiem

Darinājums ir sistēmā konstatēts fails vai objekts, kas varētu būt iesaistīts sistēmu vai tīklu zondēšanā vai uzbrukumā vai kas tiek izmantots drošības pasākumu graušanai. Darinājumi var ietvert, bet neaprobežojas ar datorvīrusiem, Trojas zirgu programmām, tārpiem, skriptiem un rīkkopām.
Darbs ar darinājumiem ietver informācijas par darinājumiem saņemšanu un to darinājumu kopiju saņemšanu, kas izmantoti uzbrukumā, spiegošanā vai citās nesankcionētās vai traucējošās darbībās. Pēc saņemšanas darinājumi tiek izpētīti. Tas ietver darinājuma rakstura, darbības mehānisma, versijas un izmantošanas analīzi un reaģēšanas pasākumu stratēģijas izstrādi (vai ieteikšanu), lai darinājumus atklātu, likvidētu un aizsargātos pret tiem. Tā kā darbu ar darinājumiem veic dažādas CSIRT vienības, izmantojot dažādas metodes, šo pakalpojumu dala sīkākās kategorijās pēc veiktās darbības un sniegtās palīdzības veida.

Darinājumu analīze

CSIRT veic sistēmā konstatēto darinājumu tehnisko pārbaudi un analīzi. Veiktā analīze var ietvert darinājuma faila veida un struktūras noteikšanu, jaunā darinājuma salīdzināšanu ar esošajiem darinājumiem vai citām tā paša darinājuma versijām, lai atklātu līdzības un atšķirības, kā arī rekonstrukciju vai koda demontāžu, lai noteiktu darinājuma nolūku un funkciju.

Reaģēšana uz darinājumiem

Šī pakalpojuma ietvaros tiek noskaidrots, kāda rīcība ir piemērota darinājumu atklāšanai un likvidēšanai sistēmā, un ar kādiem pasākumiem var novērst darinājumu instalēšanu.

Tas var ietvert parakstu izveidošanu, ko var pievienot pretvīrusu programmatūrai vai IDS.

Koordinēšana, reaģējot uz darinājumiem

Šī pakalpojuma ietvaros notiek informācijas apmaiņa ar citiem pētniekiem, CSIRT vienībām, tirgotājiem un citiem drošības speciālistiem par darinājumu analīžu rezultātiem, to sintēzi un reaģēšanas stratēģijām. Veiktie pasākumi ietver citu pušu informēšanu un no dažādiem avotiem saņemto tehnisko analīžu sintēzi. Pasākumi var ietvert arī publiska vai privāta arhīva vai datu bāzes uzturēšanu, kas satur informāciju par zināmajiem darinājumiem un atbilstošajām reaģēšanas stratēģijām.

Proaktīvie pakalpojumi

Proaktīvie pakalpojumi ir paredzēti, lai uzlabotu klientūras infrastruktūras un drošības procesus pirms incidents vai atgadījums notiek vai tiek atklāts. Galvenie mērķi ir izvairīties no incidentiem un samazināt to iedarbību un apmēru, ja tie notiek.

Paziņojumi

Tie ietver, bet neaprobežojas ar iebrukuma trauksmes ziņojumiem, ievainojamības brīdinājumiem un konsultatīvajiem drošības materiāliem. Šādi paziņojumi informē klientūras pārstāvjus par jaunām norisēm, kam būs ietekme vidējā vai ilgā laika posmā, piemēram, par jaunatklātām ievainojamībām vai iebrucēju rīkiem. Paziņojumi klientūras pārstāvjiem dod iespēju aizsargāt savas sistēmas un tīklus pret jaunatklātajām problēmām pirms to ļaunprātīgas izmantošanas.

Tehnoloģijas uzraudzīšana

CSIRT uzrauga un seko jaunākajiem tehnoloģijas sasniegumiem, iebrucēju darbībai un ar to saistītajām tendencēm, lai palīdzētu noteikt nākotnes draudus. Apskatāmās tēmas var būt plašākas, aptverot juridiskos un likumdošanas aktus, sociālos vai politiskos draudus un jaunās tehnoloģijas. Nodrošinot šo pakalpojumu, tiek lasīta drošības e-korespondence, drošības tīmekļu vietnes, jaunākās ziņas un žurnālu raksti zinātnes, tehnoloģijas, politikas un valsts pārvaldes jomā, lai iegūtu informāciju, kas attiecas uz klientūras sistēmām un tīkliem. Tas var ietvert saziņu ar citām pusēm, kas noteiktā laukā ir autoritātes, lai iegūtu labāko un precīzāko informāciju vai tās skaidrojumu. Šī pakalpojuma rezultātā var tikt sastādīts paziņojums, vadlīnijas vai rekomendācijas, kurās uzmanības tiek pievērsta vidēja termiņa vai ilgtermiņa drošības jautājumiem.

Drošības auditi vai vērtējumi

Šis pakalpojums nodrošina detalizētu vērtējumu un analīzi par organizācijas drošības infrastruktūru, pamatojoties uz organizācijas definētajām prasībām vai piemērojamiem nozares standartiem. Tas var ietvert organizācijas drošības prakses vērtēšanu. Var sniegt dažāda veida auditus un vērtējumus.

Infrastruktūras pārbaude

Manuāla aparatūras un programmatūras konfigurācijas, maršrutētāju, ugunsmūru, serveru un galda ierīču pārbaude, lai pārliecinātos, ka tie atbilst organizācijas vai nozares labākajai praksei drošības politikas jomā un standarta konfigurācijām.

Atbilstības labākai praksei pārbaude

Darbinieku un sistēmu un tīklu administratoru intervēšana, lai noskaidrotu, vai to piekoptā drošības prakse atbilst organizācijas definētajai drošības praksei vai īpašiem nozares standartiem.

Skenēšana

Ievainojamības vai vīrusi skeneru izmantošana, lai noskaidrotu, kuras sistēmas un tīkli ir ievainojami.

Iekļūšanas pārbaude

Objekta drošības pārbaude, speciāli uzbrūkot tā sistēmām un tīkliem.
Pirms šādu auditu vai vērtējumu veikšanas jāsaņem augstākās vadības atļauja. Iespējams, ka organizācijas politika dažas metodes aizliedz. Šī pakalpojuma ietvaros var izstrādāt kopēju praksi, saskaņā ar kuru veic testus un vērtējumus, kā arī izstrādāt kompetenču kopas vai sertifikācijas prasības, kas jāizpilda tiem darbiniekiem, kuri veic testēšanu, vērtēšanu, auditus vai pārbaudes. Šī pakalpojuma nodrošināšanai var izmantot arī ārpakalpojumus, ko sniedz trešās puses darbuzņēmējs vai drošības pakalpojumu sniedzējs ar atbilstošu pieredzi auditu un vērtējumu veikšanā.

Drošības rīku, lietojumprogrammu, infrastruktūru un pakalpojumu konfigurēšana un uzturēšana

Sniedzot šo pakalpojumu, tiek identificēti vai sniegti attiecīgi ieteikumi par to, kā droši konfigurēt rīkus, lietojumprogrammas un vispārējo datoru infrastruktūru, ko izmanto CSIRT klientūra vai pati CSIRT. Papildus ieteikumu sniegšanai CSIRT var veikt tādu drošības rīku un pakalpojumu kā IDS konfigurācijas veikšanu un atjaunināšanu, tīkla skenēšanu vai sistēmu, filtru, koda noteicēju, ugunsmūru, virtuālo privāto tīklu (VPT) vai autentificēšanas mehānismu uzraudzību. CSIRT pat var sniegt šos pakalpojumus kā daļu no saviem pamatpakalpojumiem. CSIRT var arī konfigurēt un uzturēt serverus, galda datorus, klēpjdatorus, personālos ciparasistentus (PDA) un citas bezvadu ierīces saskaņā ar drošības vadlīnijām. Pakalpojums ietver vadības brīdināšanu par jautājumiem vai problēmām, kas saistītas ar rīku un lietojumprogrammu konfigurāciju vai lietošanu un kas pēc CSIRT domām var padarīt sistēmu ievainojamu uzbrukuma gadījumā.

Drošības rīku izveide

Nodrošinot šo pakalpojumu, tiek izstrādāti jauni, klientiem specifiski rīki, ko pieprasa vai vēlas iegūt klientūra vai pati CSIRT. Tas var ietvert, piemēram, drošības ielāpu izveidi pielāgotai programmatūrai, ko izmanto klientūra, vai nodrošinātas programmatūras izplatīšanu, ko var izmantot skarto saimniekdatoru pārveidei. Tas var ietvert arī rīku un skriptu izstrādi, kas paplašina esošo drošības rīku funkcionalitāti, piemēram, jaunas papildprogrammas izstrādi ievainojamības vai tīkla skenerim, skripta izveidi, kas atvieglo kodēšanas tehnoloģijas izmantošanu vai automatizētu ielāpu izplatīšanas mehānismu izstrādi.

Ielaušanās atklāšanas pakalpojumi

CSIRT vienības, kas nodrošina šo pakalpojumu, izskata esošos IDS žurnālus, analizē un sāk reaģēšanas pasākumus gadījumos, kas atbilst viņu definētajam slieksnim, vai nodod trauksmes ziņojumus saskaņā ar iepriekš noteiktu pakalpojumu līmeņa līgumu vai eskalācijas stratēģiju. Iebrukumu noteikšana un ar to saistīto drošības žurnālu

analizēšana var būt ļoti sarežģīts uzdevums — vajag ne tikai noskaidrot, kurā vidē meklēt iebrukuma pazīmes, bet arī savākt un pēc tam analizēt lielu daudzumu uztverto datu. Informācijas sintēzei un interpretācijai daudzos gadījumos ir vajadzīgi speciāli rīki un zināšanas, lai noteiktu viltus trauksmes, uzbrukumus vai tīkla notikumus un lai īstenotu to likvidēšanas vai ietekmes mazināšanas stratēģijas. Lai to veiktu, dažas organizācijas izmanto ārpakalpojumus, kuru sniedzējiem, piemēram, drošības organizēšanas pakalpojumu sniedzējiem, ir plašākas speciālās zināšanas par šo pakalpojumu realizēšanu.

Ar drošību saistītas informācijas izplatīšana

Šis pakalpojums klientūrai nodrošina visaptverošu un viegli atrodamu noderīgas informācijas apkopojumu, kas palīdz uzlabot drošību. Šāda informācija var ietvert:

- ziņošanas vadlīnijas un kontaktinformāciju CSIRT vajadzībām;
- trauksmes ziņojumu, brīdinājumu un citu paziņojumu arhīvus;
- dokumentus par pašreizējo labo praksi;
- vispārējas datoru drošības vadlīnijas;
- politikas, procedūras un kontroljautājumus;
- informāciju ielāpu izveidi un izplatīšanu;
- tirgotāju saites;
- aktuālo statistiku un tendences incidentu ziņošanas jomā;
- citu informāciju, kas kopumā var uzlabot drošības praksi.

Šo informāciju var sastādīt un publicēt CSIRT vai kāda cita organizācijas nodaļa (IT, cilvēkresursu nodaļa vai preses dienests), un tā var ietvert informāciju no ārējiem avotiem, kā citām CSIRT vienībām, tirgotājiem un drošības speciālistiem.

Drošības kvalitātes vadības pakalpojumi

Pakalpojumi, kas ietilpst šajā kategorijā, nav raksturīgi tikai darbam ar incidentiem vai tikai CSIRT vienību darbībai. Tie ir labi zināmi, atzīti pakalpojumi, kas paredzēti, lai uzlabotu organizācijas drošību kopumā. Izmantojot pieredzi, kas iegūta, sniedzot iepriekš aprakstītos reaģēšanas un proaktīvas rīcības pakalpojumus, CSIRT šiem kvalitātes vadības pakalpojumiem var piešķirt jaunu perspektīvu. Šie pakalpojumi paredzēti, lai apkopotu saņemtās atsauksmes un pieredzi, balstoties uz zināšanām, kas iegūtas, reaģējot uz incidentiem, ievainojamībām un uzbrukumiem. Ar šādu pieredzi papildinot tradicionālos pakalpojumus (aprakstīti tālāk tekstā), kas tiek sniegti drošības kvalitātes vadības procesa ietvaros, var uzlabot organizācijas ilgtermiņa darbu drošības jomā. Atkarībā no organizācijas struktūras un atbildības, CSIRT var pati sniegt šos pakalpojumus vai piedalīties lielākas organizācijas kopējā darbā.
Apraksts tālāk tekstā paskaidro, ko iegūst drošības kvalitātes vadības pakalpojumi, izmantojot CSIRT speciālās zināšanas.

Riska analīze

CSIRT vienības var sniegt papildu vērtību riska analīzē un vērtējumā. Tas var uzlabot organizācijas spēju novērtēt reālos draudus, lai sniegtu reālistiskus kvalitatīvos un kvantitatīvos riska vērtējumus attiecībā uz informācijas infrastruktūru un lai novērtētu aizsardzības un reaģēšanas stratēģijas. CSIRT, kas sniedz šo pakalpojumu, veic vai palīdz veikt informācijas drošības riska analīzi jaunām sistēmām un biznesa procesiem vai novērtē pret klientūras līdzekļiem un sistēmām vērstos draudus un uzbrukumus.

Darbības nepārtrauktība un seku likvidācija

Balstoties uz iepriekšējiem atgadījumiem un nākotnes prognozēm par jaunām incidentu un drošības tendencēm, redzams, ka arvien lielāks incidentu skaits var nopietni apdraudēt drošu uzņēmuma darbu. Tāpēc, veicot plānošanu, jāņem vērā CSIRT pieredze un ieteikumi par to, kā vislabāk reaģēt uz incidentiem, lai nodrošinātu uzņēmuma darbības nepārtrauktību. CSIRT vienības, kas sniedz šo pakalpojumu, ir iesaistītas uzņēmuma darbības nepārtrauktības un avārijas seku likvidēšanas plānošanā gadījumiem, kas saistīti ar datora drošības draudiem un uzbrukumiem.

Konsultācijas drošības jautājumos

CSIRT vienības var izmantot, lai sniegtu konsultācijas un ieteikumus par labāko drošības praksi, kas ieviešama klientūras uzņēmuma darbībā. CSIRT, kas sniedz šo pakalpojumu, iesaistās rekomendāciju sagatavošanā vai nosaka prasības attiecībā uz jaunu sistēmu, tīkla ierīču, lietojumprogrammu vai visa uzņēmuma biznesa procesu ieviešanu, instalēšanu vai nodrošināšanu. Šis pakalpojums ietver ieteikumu sniegšanu un palīdzību, izstrādājot organizācijas vai klientūras drošības politiku. Tas var būt saistīts arī ar pierādījumu vai konsultāciju sniegšanu likumdošanas vai citām valsts pārvaldes iestādēm.

Izpratnes veidošana

CSIRT var būt iespēja noskaidrot, kādās jomās klientūras pārstāvjiem vajag vairāk informācijas un ieteikumu, lai labāk izpildītu pieņemtās drošības prakses un organizācijas drošības politikas prasības. Labāka klientūras vispārējā informētība par drošību ne tikai uzlabo viņu sapratni par drošības jautājumiem, bet arī palīdz tiem pildīt ikdienas darbu drošākā veidā. Tas var samazināt sekmīgo uzbrukumu skaitu un palielināt izredzes, ka klientūras pārstāvji atklās uzbrukumus un ziņos par tiem, tādējādi samazinot seku likvidēšanas laiku un novēršot vai samazinot zaudējumus.
CSIRT, kas nodrošina šos pakalpojumus, meklē iespējas veicināt informētību par drošību, veidojot rakstus, plakātus, informatīvos izdevumus, tīmekļa vietnes vai citus informācijas resursus, kas izskaidro, kāda ir laba drošības prakse, un sniedz padomus par veicamajiem piesardzības pasākumiem. Var rīkot arī sapulces un seminārus, lai informētu klientūru par jaunākajām drošības procedūrām un potenciālajiem sistēmu draudiem to organizācijas jomā.

Izglītība, apmācība

Šī pakalpojuma ietvaros klientūras pārstāvjiem tiek sniegta informācija par datoru drošības jautājumiem, izmantojot seminārus, darba seminārus, kursus un konsultācijas. Apskatāmās tēmas var iekļaut incidentu paziņošanas vadlīnijas, atbilstošas reaģēšanas metodes, incidentu reaģēšanas rīkus, incidentu novēršanas metodes un citu informāciju, kas nepieciešama, lai aizsargātos pret datoru drošības incidentiem, tos atklātu, ziņotu par tiem un reaģētu uz tiem.

Produktu vērtēšana vai sertifikācija

Sniedzot šo pakalpojumu, CSIRT veic produktu vērtēšanu attiecībā uz rīkiem un lietojumprogrammām vai sniedz citus pakalpojumus, lai panāktu produktu drošību un to atbilstību CSIRT vai organizācijas pieņemtajai drošības praksei. Pārbaudāmie rīki vai lietojumprogrammas var būt ar atklāto pirmkodu vai komerciāli produkti. Šo pakalpojumu

var sniegt kā vērtēšanas pakalpojumu vai arī kā sertificēšanas programmu — tas atkarīgs no organizācijas vai CSIRT izmantotajiem standartiem.

A.3. Piemēri

Fiktīvā CSIRT

0. uzdevums — izpratne par to, kas ir CSIRT

Paraugā minētā CSIRT apkalpo vidēja lieluma iestādi, kurā strādā 200 darbinieki. Šai iestādei ir sava IT nodaļa un divas filiāles, kas atrodas tai pašā valstī. Šajā uzņēmumā IT ir būtiska loma, jo to izmanto iekšējai saziņai, datu tīklam un 24x7 e-darījumiem. Iestādei ir savs tīkls un rezerves pieslēgums internetam, un tā saņem pakalpojumus no diviem atšķirīgiem interneta pakalpojumu sniedzējiem.

- -

1. uzdevums — sākuma posms

Sākuma posmā jaunā CSIRT tiek plānota kā iekšēja CSIRT, kas sniedz pakalpojumus mītnes uzņēmumam, vietējai IT nodaļai un darbiniekiem. Tā arī atbalsta un koordinē rīcību starp dažādām filiālēm IT drošības incidentu gadījumā.

- -

2. uzdevums — piemērotu pakalpojumu izvēle

Sākuma posmā tiek nolemts, ka jaunās CSIRT vienības darbība koncentrēsies galvenokārt uz pamatpakalpojumu sniegšanu darbiniekiem.

Tiek nolemts, ka pakalpojumu klāsta paplašināšana tiks apsvērta pēc izmēģinājuma posma un, iespējams, tiks piedāvāti arī drošības pārvaldības pakalpojumi. Lēmums tiks pieņemts, balstoties uz komentāriem, ko sniegs izmēģinājuma posma klientūra, un ciešā sadarbībā ar kvalitātes nodrošināšanas nodaļu.

- -

3. uzdevums — klientūras un piemēroto komunikācijas kanālu analizēšana

Piedaloties svarīgākajiem vadības un klientūras pārstāvjiem, ideju ģenerēšanas sesijā tiek iegūta pietiekama informācija SVID analīzei. Analīzes rezultātā tiek secināts, ka nepieciešami šādi pamatpakalpojumi:

- trauksmes paziņojumi un brīdinājumi
- darbs ar incidentiem (analīze, atbalsts un koordinācija, reaģējot uz incidentu)
- paziņojumi

Ir jānodrošina, lai informācijas izplatīšana tiktu labi organizēta, sasniedzot maksimāli lielu klientūras daļu. Tāpēc tiek pieņemts lēmums, ka trauksmes, brīdinājumi un paziņojumi tiks publicēti konsultatīvo drošības materiālu formā specializētā tīmekļa vietnē un izsūtīti sarakstā iekļautiem e-pasta adresātiem. Incidentu ziņojumu saņemšanai CSIRT izmantos arī e-pastu, telefonu un faksu. Nākamais uzdevums paredz vienotas tīmekļa veidlapas izveidi.

4.uzdevums — misijas formulējums

Fiktīvās CSIRT vadība ir uzrakstījusi šādu misijas formulējumu:
„Izdomātā CSIRT sniedz informāciju un palīdzību mītnes organizācijas darbiniekiem, lai samazinātu datoru drošības incidentu risku, kā arī lai reaģētu uz incidentiem, kad tie notiek.”

Līdz ar to fiktīvā CSIRT skaidri nosaka, ka tā ir uzņēmuma iekšēja CSIRT un ka tās pamatnodarbošanās ir IT drošības jautājumi.

- -

5. uzdevums — biznesa plāna sastādīšana

Finanšu modelis
Tā kā uzņēmums nodrošina 24x7 e-darījumu pakalpojumus un tam ir IT nodaļa, kas strādā 24x7 režīmā, tiek nolemts sniegt pilnus pakalpojumus darba laikā un ārpus parastā darba laika strādāt pēc izsaukuma. Klientūrai pakalpojumi tiks sniegti bez maksas, bet iespēja sniegt pakalpojumus klientiem ārpus uzņēmuma tiks apsvērta izmēģinājuma un vērtēšanas posmā.

Ienākumu modelis
Darbības sākuma un izmēģinājuma posmā CSIRT finansēs mītnes uzņēmums. Izmēģinājuma un novērtēšanas posma laikā tiks apspriesta papildu finansēšana, ieskaitot iespēju pārdot pakalpojumus klientiem ārpus uzņēmuma.

Organizācijas modelis
Mītnes uzņēmums ir neliels uzņēmums, tāpēc tiek izvēlēts iegultais modelis.
Darba laikā trīs darbinieki sniegs pamatpakalpojumus (izplatīs konsultatīvos drošības materiālus, strādās ar incidentiem un veiks koordinēšanu).

Uzņēmuma IT nodaļa jau nodarbina cilvēkus ar atbilstošām iemaņām. Ar nodaļu tiek panākta vienošanās, ka jaunā CSIRT vienība pēc vajadzības var lūgt tās atbalstu. Turklāt var izmantot tās 2. līmeņa izsaukuma tehniķus.
CSIRT vienībā būs 4 pilna darba laika dalībnieki un 5 papildu dalībnieki. Viens no tiem strādās maiņās rotācijas kārtībā.

Darbinieki
CSIRT vienības vadītājam ir pieredze drošības darbā, sniedzot 1. un 2. līmeņa atbalstu, un viņš ir strādājis krīzes seku likvidēšanas pārvaldības jomā. Pārējie trīs vienības dalībnieki ir drošības speciālisti. Nepilnas slodzes CSIRT vienības dalībnieki, kas piesaistīti no IT nodaļas, ir uzņēmuma infrastruktūras speciālisti.

5. uzdevums — biroja telpu izmantošana un informācijas drošības politika

Biroja iekārtas un izvietojums
Tā kā mītnes organizācijai jau ir efektīva fiziskā drošība, šai ziņā jaunā CSIRT ir labi sagatavota. Tiek atvēlēta tā saucamā „kara telpa”, lai ārkārtas gadījumos varētu veikt koordinēšanu. Šifrēto materiālu un slepeno dokumentu glabāšanai ir iegādāts seifs. Ir iekārtota atsevišķa telefona līnija ar komutatoru karstās līnijas vajadzībām darba laikā un mobilais telefons ar tādu pašu numuru izsaukumiem ārpus parastā darba laika.

Lai paziņotu ar CSIRT saistītu informāciju, var izmantot arī esošo aprīkojumu un uzņēmuma tīmekļa vietni. Tiek instalēta un uzturēta adresātu saraksta programmatūra ar ierobežotu sadaļu saziņai ar vienības dalībniekiem un citām vienībām. Visa darbinieku kontaktinformācija tiek glabāta datu bāzē, tās izdruka atrodas seifā.

Noteikumi
Tā kā CSIRT strādā uzņēmuma ietvaros, kurā jau pastāv informācijas drošības politika, attiecīgie CSIRT drošības noteikumi tiek izveidoti ar uzņēmuma juriskonsulta palīdzību.
- -
7. uzdevums — sadarbības iespēju meklēšana
Izmantojot ENISA Uzskaiti, valstī ātri tiek atrastas citas CSIRT vienības, un ar tām tiek nodibināti kontakti. Tiek panākta vienošanās, ka vienu no tām apmeklēs tikko darbā pieņemtais vienības vadītājs. Viņš iepazīstas ar CSIRT aktivitātēm valstī un apmeklē vienu sapulci.
Sapulcē apskatītie darba metožu paraugi un citu vienību piedāvātā palīdzība ir ļoti noderīga.
8. uzdevums — biznesa plāna virzīšana

Tiek nolemts apkopot faktus un skaitļus par uzņēmuma vēsturi. Tas sniedz ļoti noderīgu statistisku pārskatu par IT drošības situāciju. Šo apkopojumu vajag turpināt pēc CSIRT izveides, lai šo statistiku aktualizētu.

Tiek nodibināti sakari ar citām CSIRT vienībām valstī, lai apspriestu to darbības pamatojumus. Vienības sniedz atbalstu, izveidojot slaidus ar informāciju par jaunākajiem notikumiem IT drošības incidentu jomā un incidentu radītajām izmaksām.

Šajā izdomātās CSIRT vienības piemērā nebija aktuālas vajadzības pārliecināt vadību par IT nozares svarīgumu, un tāpēc gūt atbalstu pirmā posma uzsākšanai nebija grūti. Tiek sagatavots darbības pamatojums un projekta plāns, ieskaitot vienības izveides izmaksu aprēķinu un darbības izmaksas.
- -

9. uzdevums — procesu norises, operatīvo un tehnisko procedūru noteikšana
Fiktīvā CSIRT koncentrējas uz CSIRT pamatpakalpojumu sniegšanu:

- trauksmes ziņojumi un brīdinājumi
- paziņojumi
- darbs ar incidentiem

Vienība izstrādā procedūras, kas labi funkcionē un ir viegli saprotamas visiem vienības locekļiem. Izdomātā CSIRT pieņem darbā arī juristu, kas nodarbojas ar tiesiskās atbildības jautājumiem un informācijas drošības politiku. Apspriežoties ar citām CSIRT vienībām, jaunā vienība apgūst lietderīgus rīkus un iegūst noderīgu informāciju par operatīviem jautājumiem.

Tiek izveidota noteikta veidne konsultatīvo drošības materiālu un incidentu ziņojumu sastādīšanai. Darbam ar incidentiem vienība izmanto RTIR.

- -

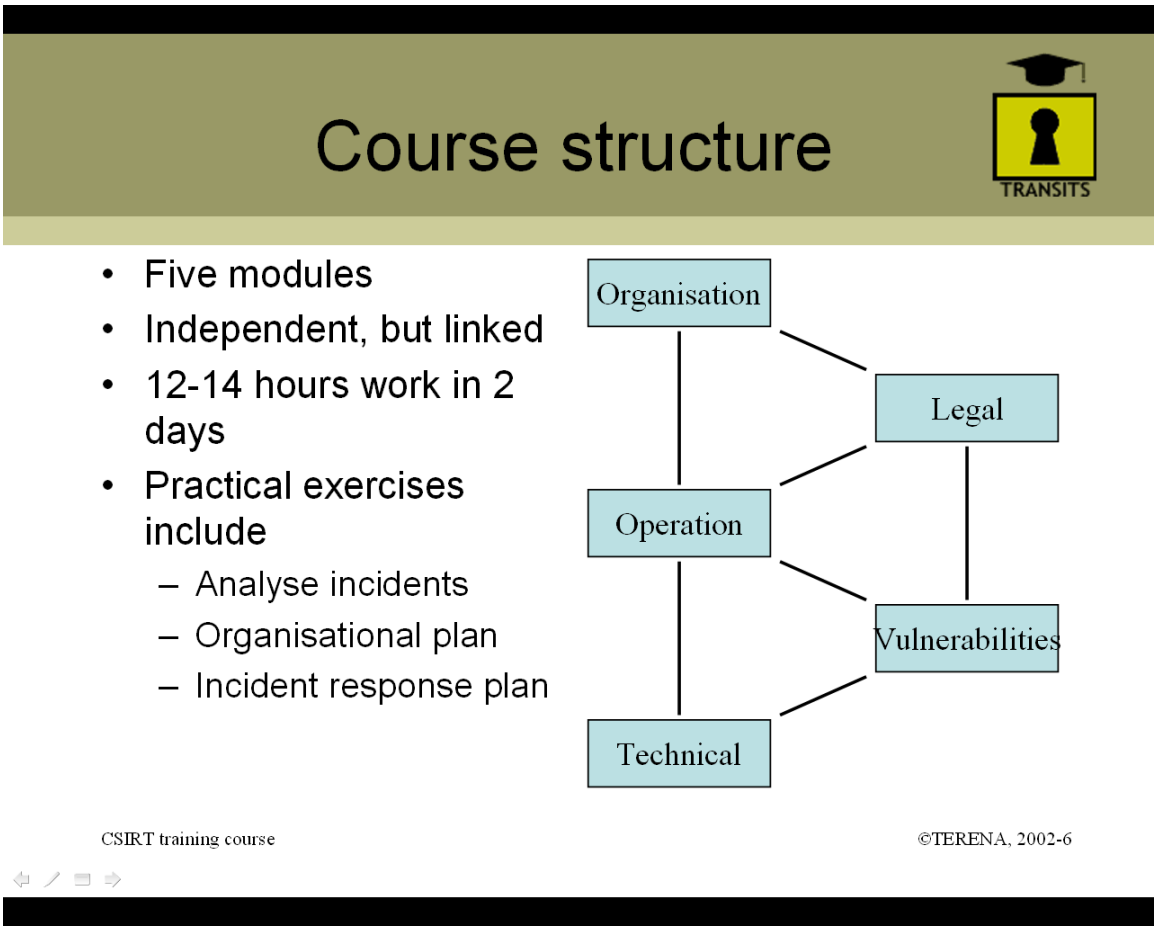
10. uzdevums — darbinieku apmācība
Fiktīvā CSIRT nolemj nosūtīt savus tehniskos darbiniekus uz nākamajiem TRANSITS kursiem. Turklāt vienības vadītājs apmeklē CERT/CC kursu par CSIRT vadīšanu.

- -

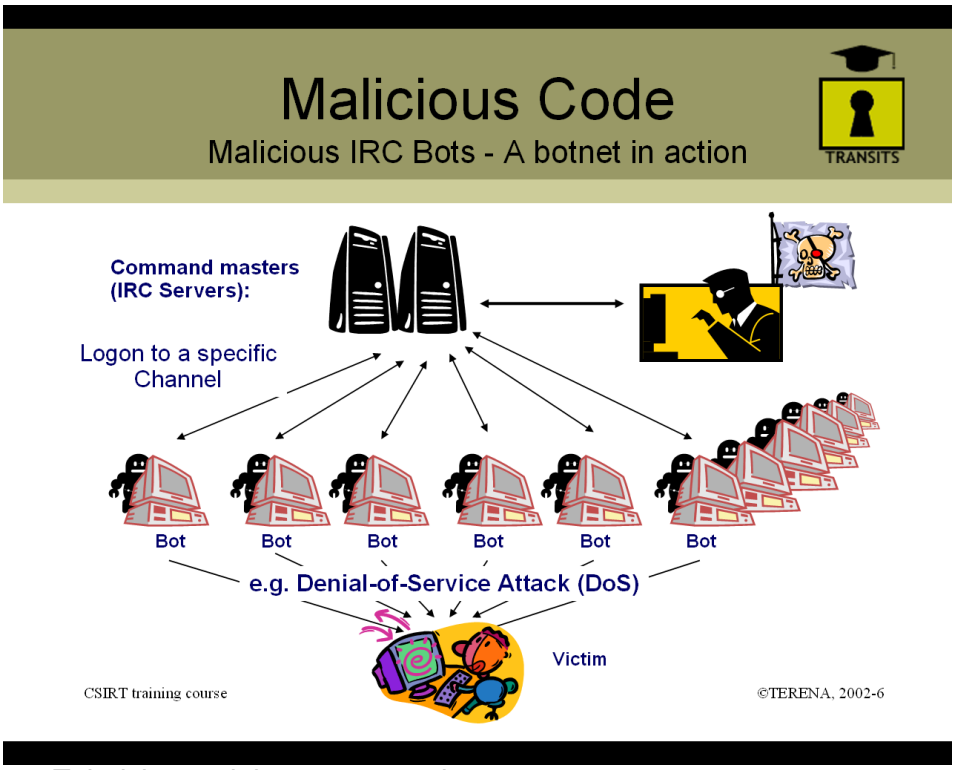
11. uzdevums — vingrinājumi
Darbības pirmajā nedēļā fiktīvā CSIRT vingrinājumiem izmanto vairākus izdomātus gadījumus (tos viņi piemēru veidā dabū no citām CSIRT vienībām). Turklāt viņi izdod pāris konsultatīvos drošības materiālus, balstoties uz aparatūras un programmatūras pārdevēju izplatīto informāciju par īstām ievainojamībām, ko viņi pielāgo savas klientūras vajadzībām.

A.4. Materiālu paraugi no CSIRT kursiem

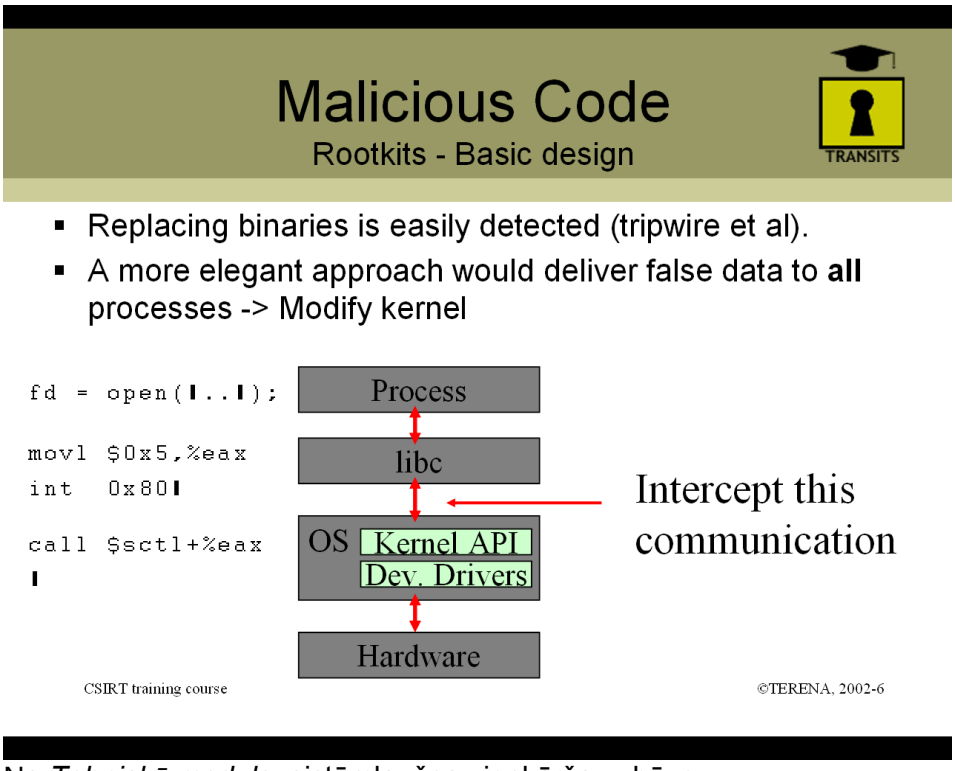
TRANSITS (ar Terena laipnu atļauju (http://www.terena.nl)



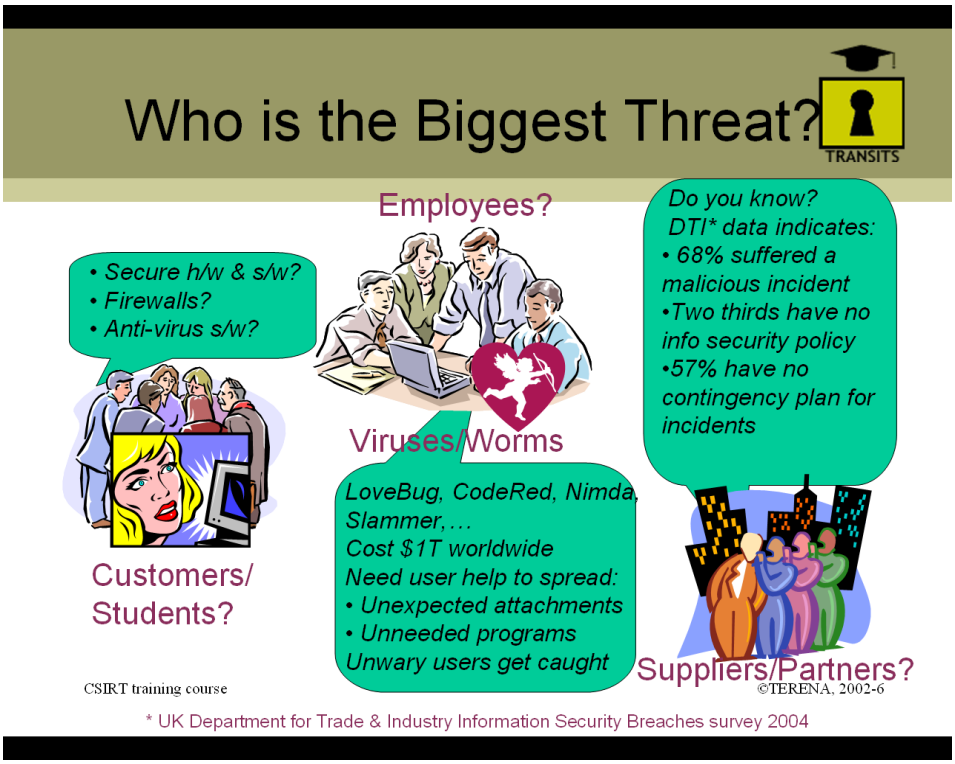
Pārskats: kursa struktūra



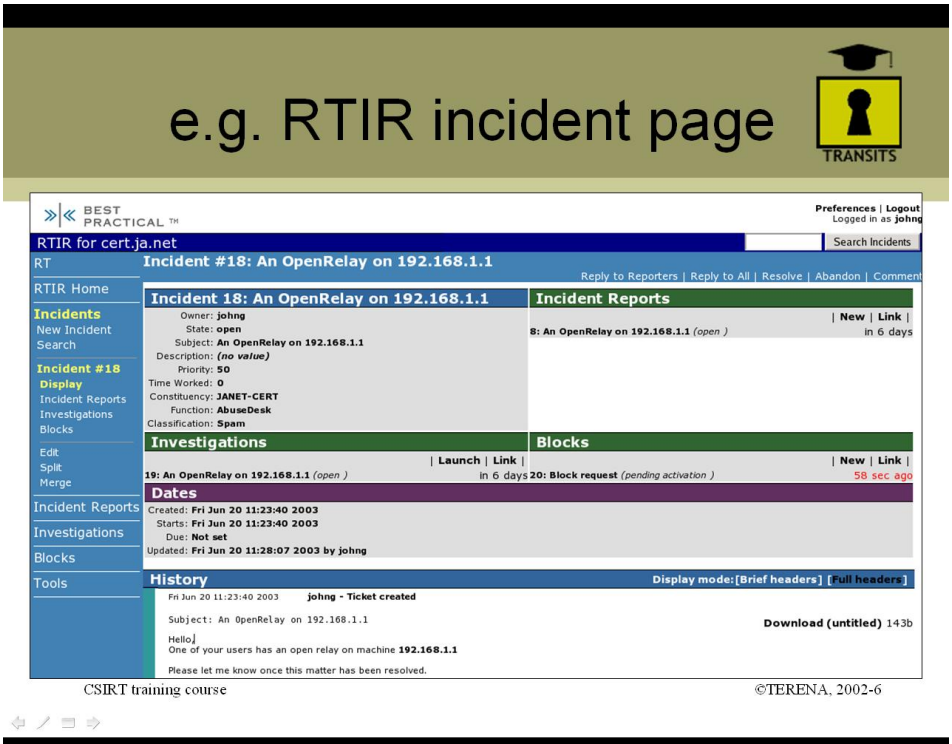
No *Tehniskā moduļa:* Botnet apraksts



No *Tehniskā moduļa:* sistēmlaužņa vienkārša uzbūve



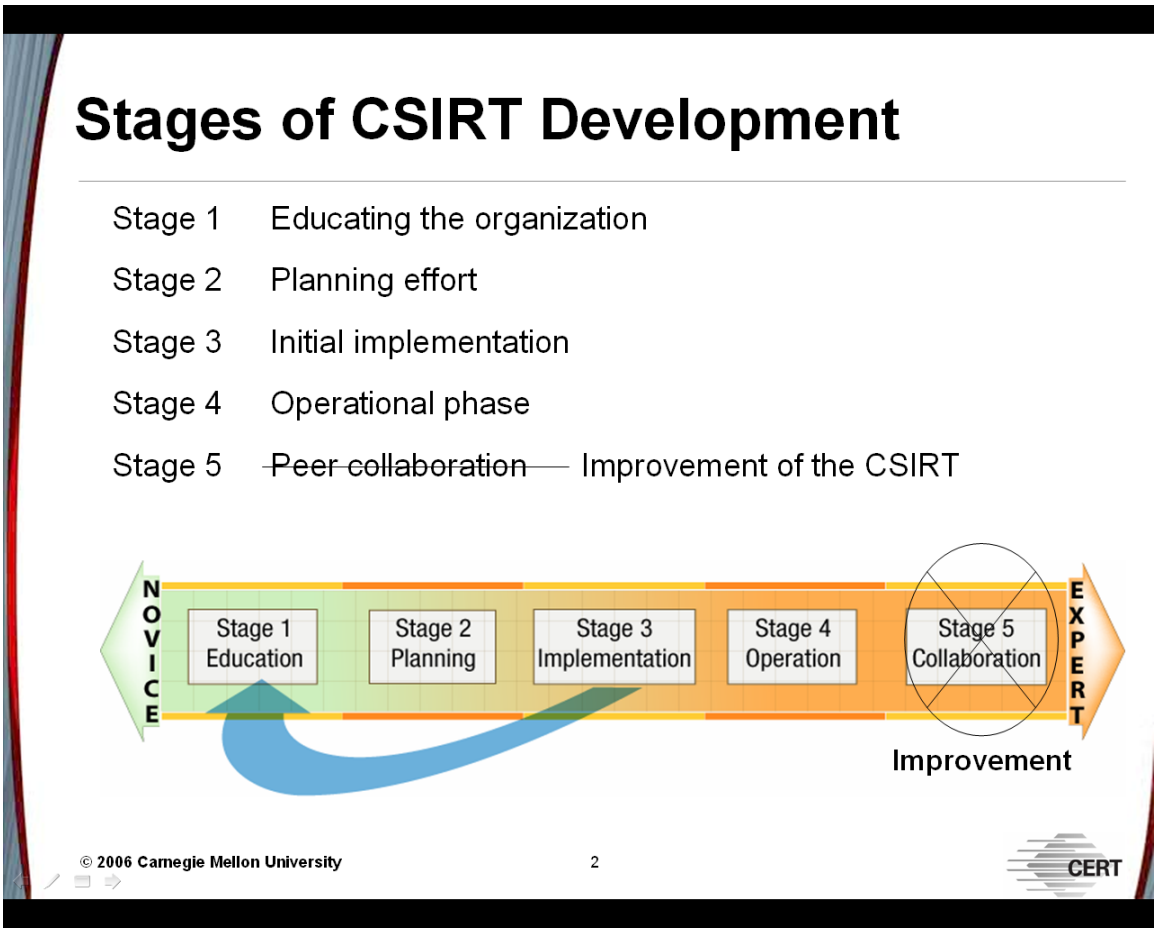
No *Organizatoriskā moduļa:* savējais vai svešinieks - kas rada lielākus draudus



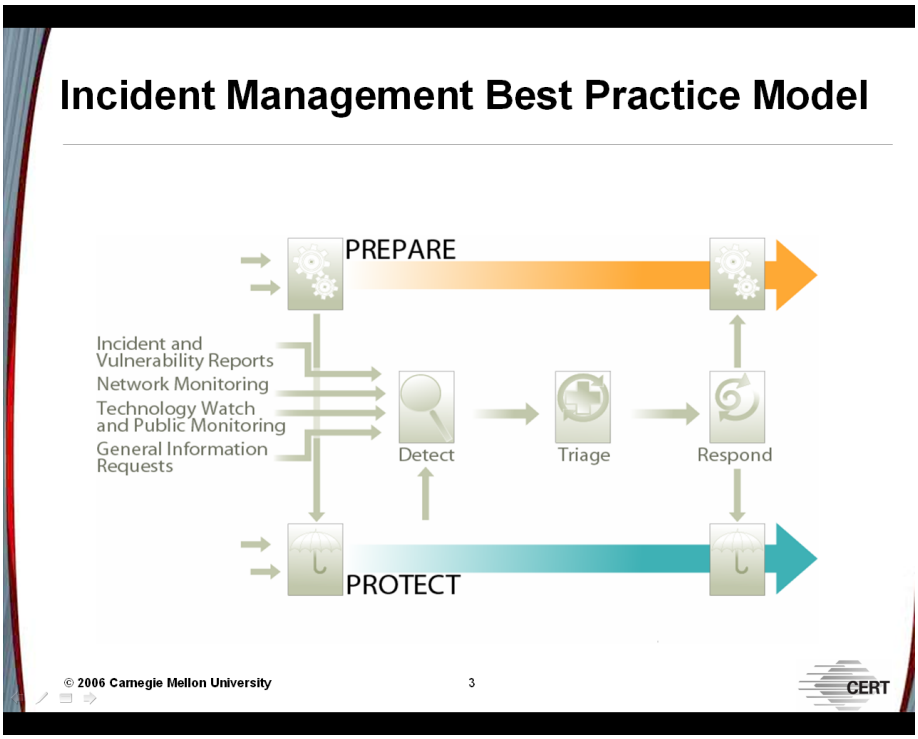
No *Operāciju gaitas: Request Tracker for Incident Response* (trekera pieprasīšana reaģēšanai uz incidentu — RTIR)

„CSIRT vienību izveide" (ar laipnu CERT/CC atļauju, http://www.cert.org)

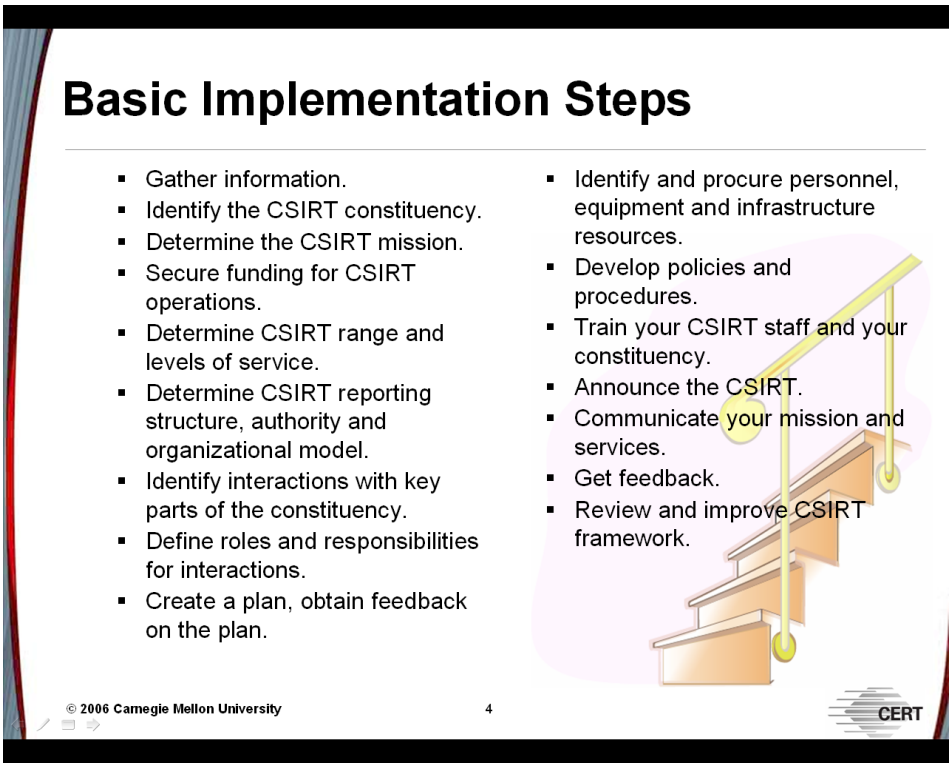
ENISA pateicas CSIRT programmas CSIRT izveides vienībai par atļauju izmantot apmācības kursu materiālu!



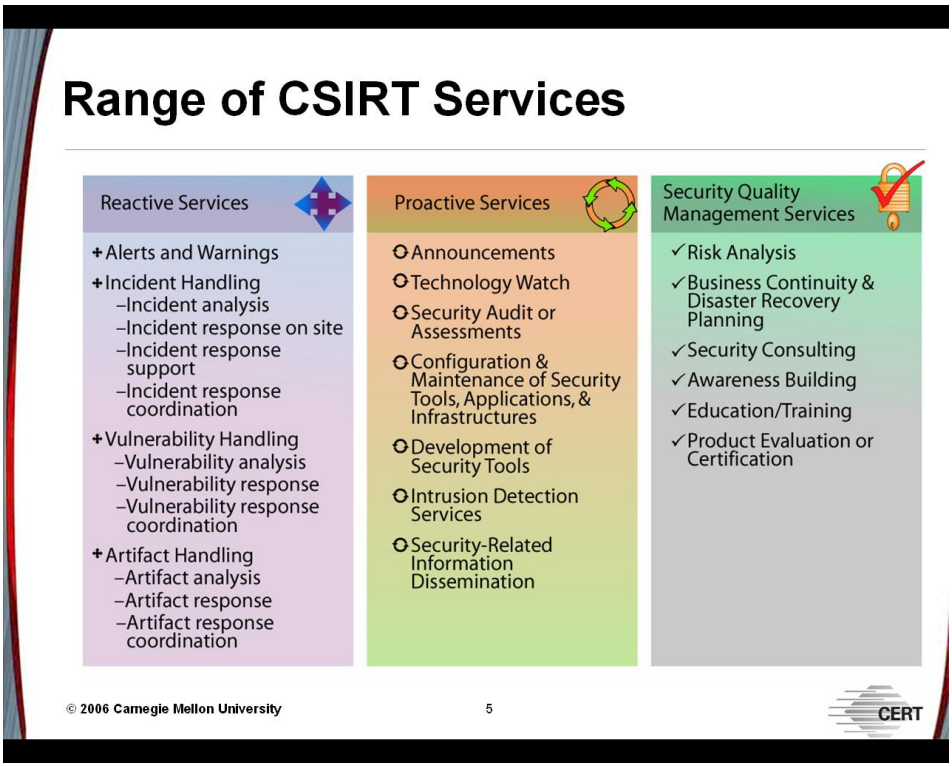
No *CERT/CC apmācības kursa:* CSIRT attīstības posmi



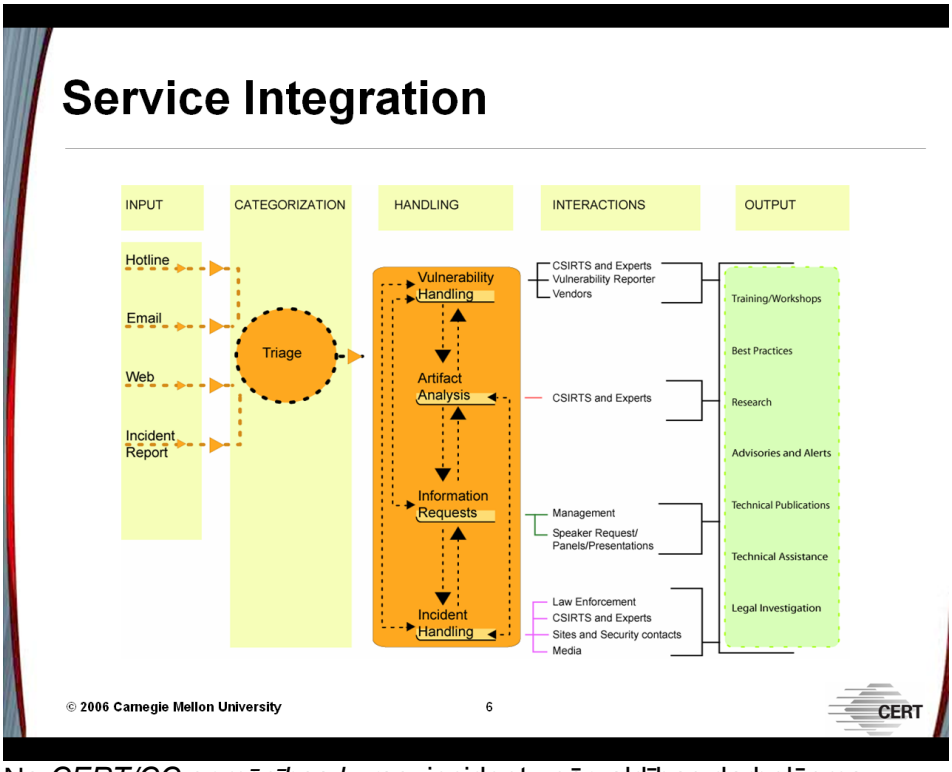
No *CERT/CC apmācības kursa:* laba incidentu pārvaldības prakse



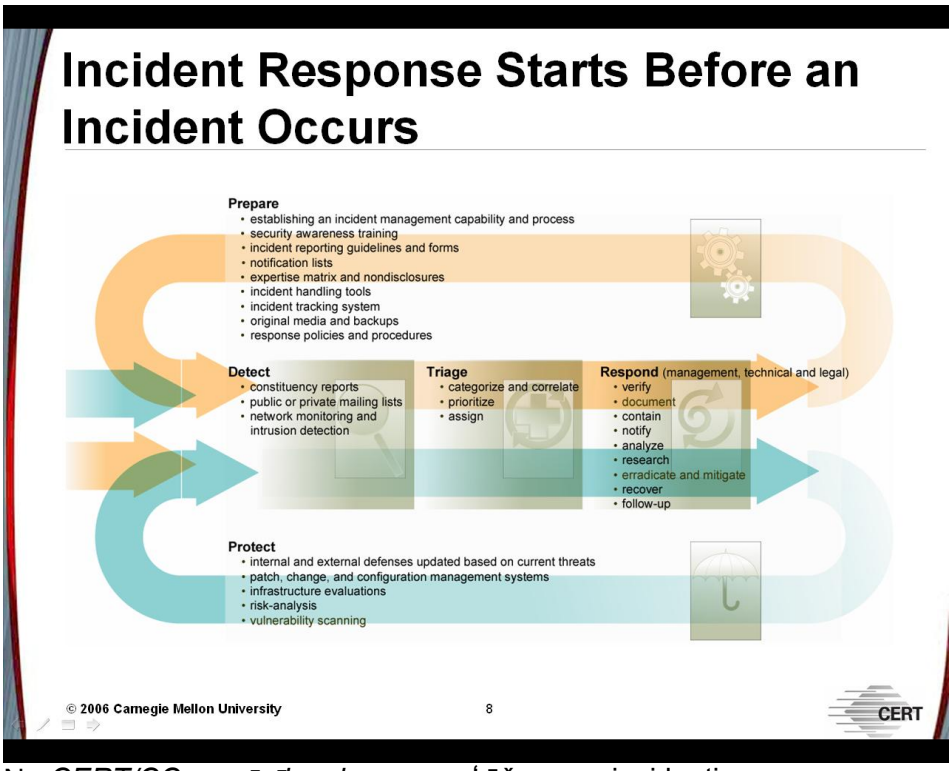
No *CERT/CC apmācības kursa:* CSIRT izveides posmi



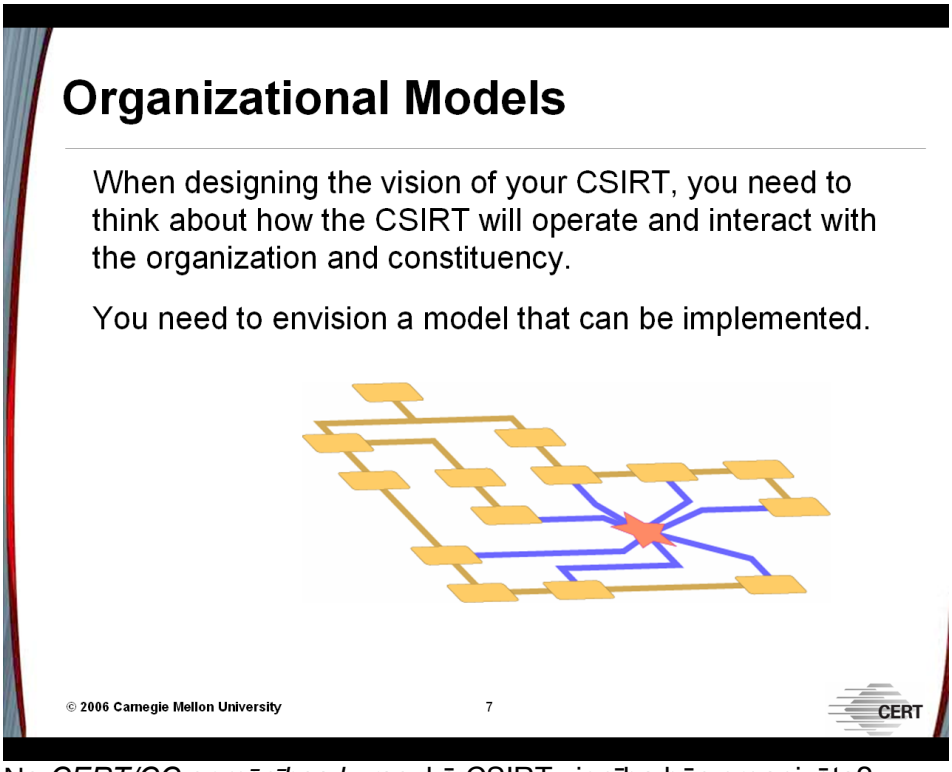
No *CERT/CC apmācības kursa:* pakalpojumi, ko var sniegt CSIRT



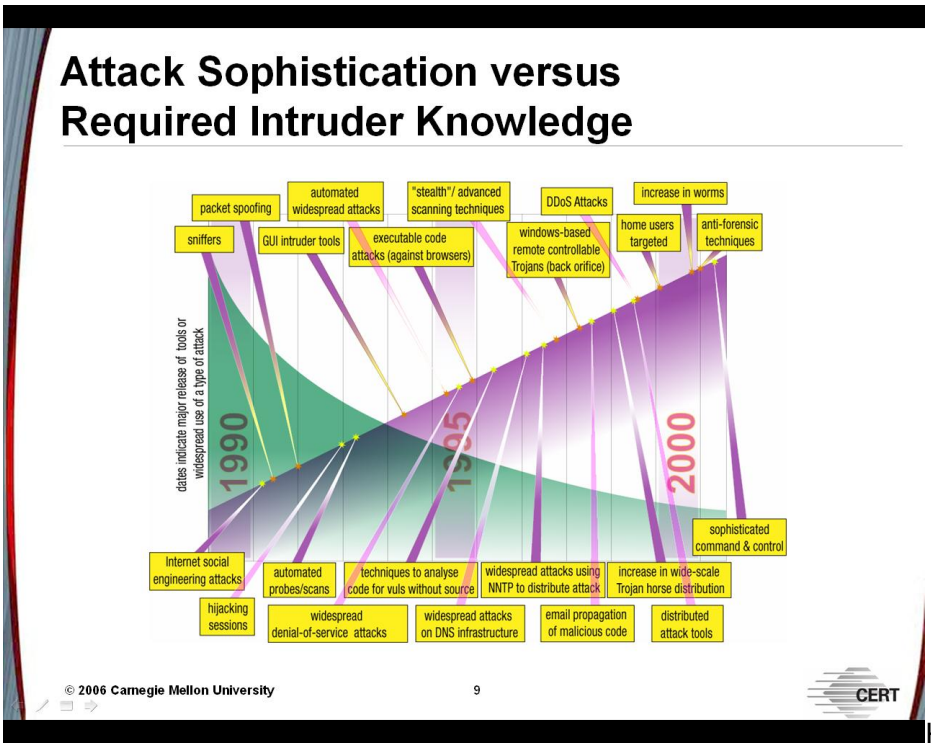
No *CERT/CC apmācības kursa:* incidentu pārvaldības darbplūsma



No *CERT/CC apmācības kursa:* reaģēšana uz incidentiem



No *CERT/CC apmācības kursa:* kā CSIRT vienība būs organizēta?


K

No *CERT/CC apmācības kursa:* mazāk zināšanu, lielāks posts