APPROĊĊ PASS PASS DWAR KIF TWAQQAF CSIRT

Dokument WP2006/5.1(CERT-D1/D2)

Werrej

1 Sommarju Amministrattiv

Dan id-dokument jiddeskrivi l-proċess tat-twaqqif ta' Tim ta' Rispons dwar is-Sigurtà u l-Inċidenti tal-Kompjuter (CSIRT – *Computer Security and Incidence Response Team*) mill-perspettivi rilevanti kollha bħall-immaniġġjar tan-negozju, l-immaniġġjar tal-proċessi u l-perspettiva teknika. Dan id-dokument jimplimenta tnejn mid-dokumenti deskritti fil-Programm ta' Ħidma ta' ENISA 2006, kapitolu 5.1;

- Dan id-dokument: *Rapport bil-miktub fuq approċċ pass pass dwar kif twaqqaf CERT jew faċilitajiet simili, fosthom eżempji.*(**CERT-D1**)
- Kapitolu 12 u fajls esterni: *Estratt mir-roadmap f'forma dettaljata li jippermetti applikazzjoni faċli tar-roadmap fil-prattika.* (**CERT-D2**)

2 Avviż Legali

Wieħed għandu jinnota li din il-pubblikazzjoni tirrappreżenta l-opinjonijiet u l-interpretazzjonijiet ta' l-awturi u l-edituri, sakemm ma jkunx sostnut mod ieħor. Din il-pubblikazzjoni m'għandhiex tittieħed bħala azzjoni ta' ENISA jew l-organi ta' ENISA sakemm ma tkunx adottata skond ir-Regolament ta' ENISA (KE) Nru 460/2004. Din il-pubblikazzjoni mhux neċessarjament tirrappreżenta l-aħħar żviluppi u tista' tiġi aġġornata minn żmien għall-ieħor.

Sorsi ta' partijiet terzi huma kkwotati kif jixraq. ENISA mhix responsabbli għall-kontenut tas-sorsi esterni fosthom websajts esterni li hemm referenza għalihom f'din il-pubblikazzjoni.

Din il-pubblikazzjoni hija intenzjonata għal skopijiet edukattivi u ta' informazzjoni biss. La ENISA u ebda persuna li taġixxi f'isimha ma hija responsabbli għall-użu li jista' jsir mill-informazzjoni kontenuta f'din il-pubblikazzjoni.

Id-drittijiet kollha huma miżmuma. L-ebda parti minn din il-pubblikazzjoni ma tista' tiġi kkupjata, maħżuna f'sistema ta' rkupru jew trasmessa fi kwalunkwe forma jew bi kwalunkwe mezz, elettroniku mekkaniku, fotokopjar, irrekordjar, jew mod ieħor mingħajr il-permess bil-miktub minn quddiem ta' ENISA, jew kif espressament permess bil-Liġi jew skond it-termini miftiehma ma' l-organizzazzjonijiet xierqa għad-drittijiet. Is-sors irid jiġi rikonoxxut f'kull ħin. It-talbiet għar-riproduzzjoni jistgħu jintbagħtu lill-indirizz ta' kuntatt ikkwotat f'din il-pubblikazzjoni.

3 Rikonoxximenti

ENISA tixtieq tirringrazzja lill-istituzzjonijiet u lill-persuni kollha li kkontribwew għal dan id-dokument. "Grazzi" speċjali jmur għal dawn il-kontributuri:

- Henk Bronk, li bħala konsulent ipproduċa l-ewwel verżjoni ta' dan id-dokument.
- Il-CERT/CC u speċjalment it-tim għall-iżvilupp tal-CSIRT, li kkontribwixxa materjal utli ħafna u l-materjal kampjun tal-kors fl-anness.
- GovCERT.NL talli pprovda *CERT-f'kaxxa*
- It-tim TRANSITS li kkontribwixxa l-materjal kampjun tal-kors fl-anness.

- Il-kollegi mit-taqsima għall-Politika dwar is-Sigurtà fid-Dipartiment Tekniku li kkontribwew kapitolu 6.6
- In-numru bla għadd ta' persuni li rrevedew dan id-dokument

4 Introduzzjoni

In-netwerks ta' komunikazzjoni u s-sistemi ta' informazzjoni saru fattur importanti fl-iżvilupp ekonomiku u soċjali. L-informatika u n-netwerking illum qed isiru utilitajiet li ssibhom kullimkien bl-istess mod bħalma hija l-provvista ta' l-elettriku jew ta' l-ilma.

Is-sigurtà tan-netwerks ta' komunikazzjoni u tas-sistemi ta' informazzjoni u d-disponibilità tagħhom b'mod partikolari, għalhekk hija ta' interess dejjem akbar għas-soċjetà. Dan jirriżulta mir-riskju ta' problemi f'sistemi vitali ta' informazzjoni, minħabba l-kumplessità tas-sistema, aċċidenti, żbalji u attakki għall-infrastrutturi fiżiċi li jwasslu servizzi essenzjali għall-benesseri taċ-ċittadini ta' l-UE.

Fl-10 ta' Marzu 2004 ġiet stabbilita Aġenzija Ewropea dwar is-Sigurtà tan-Netwerks u l-Informazzjoni (ENISA)[1]. L-għan tagħha huwa li tassigura livell għoli u effettiv tan-netwerk u l-informazzjoni fi ħdan il-komunità u li tiżviluppa kultura ta' sigurtà fin-netwerk u l-informazzjoni għall-benefiċċju taċ-ċittadini, il-konsumaturi, l-intrapriżi u l-organizzazzjonijiet tas-settur pubbliku fi ħdan l-Unjoni Ewropea, biex hekk tikkontribwixxi għall-funzjonament bla problemi tas-suq intern.

Għal diversi snin issa, numru ta' komunitajiet tas-sigurtà fl-Ewropa bħal CERT/CSIRTs, Timijiet kontra l-Abbużi u WARPs ikkollaboraw għal Internet aktar sigur. ENISA beħsiebha tappoġġja 'l dawn il-komunitajiet fl-isforzi tagħhom billi tipprovdi informazzjoni dwar miżuri sabiex jiġi assigurat livell xieraq ta' kwalità tas-servizz. Barra minn hekk ENISA beħsiebha ttejjeb il-kapaċità tagħha li tagħti parir lill-istati membri ta' l-UE u lill-organi ta' l-UE fi kwistjonijiet tal-kopertura ta' gruppi speċifiċi ta' utenti ta' l-IT b'servizzi xierqa ta' sigurtà. Għalhekk, billi jibni fuq is-sejbiet tal-Grupp ta' Ħidma *ad hoc* CERT Kooperazzjoni u Appoġġ, stabbilit fl-2005, dan il-Grupp ta' Ħidma ġdid se jittratta kwistjonijiet li għandhom x'jaqsmu ma' l-għoti ta' servizzi adegwati tas-sigurtà ("servizzi CERT") lil (kategoriji jew gruppi) speċifiċi ta' utenti.

ENISA tappoġġja t-twaqqif ta' CSIRTs ġodda bil-pubblikazzjoni ta' dan ir-rapport ta' ENISA "*Approċċ pass pass dwar kif twaqqaf CSIRT b'lista ta' kontroll supplimentari*", li għandu jgħinek twaqqaf il-CSIRT tiegħek.

[1] Regolament (KE) Nru 460/2004 tal-Parlament Ewropew u tal-Kunsill ta' l-10 ta' Marzu 2004 li jistabbilixxi l-Aġenzija Ewropea dwar is-Sigurtà tan-Netwerks u l-Informazzjoni. "Aġenzija tal-Komunità Ewropea" tfisser organu mwaqqaf mill-UE biex iwettaq kompitu tekniku, xjentifiku jew amministrattiv speċifiku ħafna fl-"isfera tal-Komunità" ("l-ewwel pilastru") ta' l-UE.

Udjenza fil-Mira

Il-gruppi fil-mira prinċipali għal dan ir-rapport huma istituzzjonijiet governattivi u oħrajn li jiddeċiedu li jwaqqfu CSIRT bil-għan li jipproteġu l-infrastruttura ta' l-IT tagħhom stess jew dik tal-partijiet interessati tagħhom.

Kif tuża dan id-dokument

Dan id-dokument se jipprovdi informazzjoni dwar x'inhu CSIRT, x'servizzi jista' jipprovdi u x'inhuma l-passi meħtieġa biex tibda. Dan għandu jagħti lill-qarrej ħarsa ġenerali tajba u pragmatika ta' l-approċċ, l-istruttura u l-kontenut dwar kif twaqqaf CSIRT.

Kapitlu 4 *"Introduzzjoni"*
Introduzzjoni għal dan ir-rapport

Kapitlu 5 *"Strateġija ġenerali għall-ippjanar u t-twaqqif ta' CSIRT"*
L-ewwel parti tagħti deskrizzjoni ta' x'inhu CSIRT. Hija għandha tipprovdi wkoll informazzjoni dwar l-ambjenti differenti li fih jistgħu jaħdmu l-CSIRTs u x'servizzi jistgħu jagħtu.

Kapitlu 6 *"Żvilupp tal-Pjan Korporattiv"*
Dan il-kapitlu jiddeskrivi l-approċċ ta' immaniġġjar korporattiv lejn i-proċess tat-twaqqif.

Kapitlu 7 *"Promozzjoni tal-Pjan Korporattiv"*
Dan il-kapitlu jittratta l-każ korporattiv u kwistjonijiet ta' fondi.

Kapitlu 8 *"Eżempji ta' proċeduri operattivi u tekniċi"*
Dan il-kapitlu jiddeskrivi l-proċedura tal-ksib ta' l-informazzjoni u jittraduċiha f'bullettin tas-sigurtà. Dan il-kapitlu jipprovdi wkoll deskrizzjoni ta' fluss tax-xogħol għall-ġestjoni ta' inċident.

Kapitlu 9 *"Taħriġ tal-CSIRT"*
Dan il-kapitlu jagħti sommarju tat-taħriġ disponibbli tal-CSIRT. Bħala eżempju, fl-anness hemm ipprovdut materjal kampjun tal-kors.

Kapitlu 10 *"Eżerċizzju: produzzjoni ta' konsulta"*
Dan il-kapitlu fih eżerċizzju dwar kif twettaq wieħed mis-servizzi bażiċi (jew ċentrali) tal-CSIRT: il-produzzjoni ta' bulletin tas-sigurtà (jew konsulta).

Kapitlu 12 "Deskrizzjoni tal-Pjan tal-Proġett"
Dan il-kapitlu jirreferi għall-pjan tal-proġett supplimentari (lista ta' kontroll) pprovdut ma' din il-gwida. Dan il-pjan għandu l-mira li jkun għodda faċli biex tużaha għall-implimentazzjoni ta' din il-gwida.

Konvenzjonijiet użati f'dan id-dokument

Biex jiggwida lill-qarrej, kull kapitlu jibda b'sommarju tal-passi meħuda sa issa fil-proċess tat-twaqqif ta' CSIRT. Dawn is-sommarji huma mogħtija f'kaxxi bħal din li ġejja:

Għamilna l-ewwel pass

Kull kapitlu jispiċċa b'eżempju prattiku tal-passi diskussi. F'dan id-dokument, il-"CSIRT Fittizju" se jkun CSIRT żgħir indipendenti għal kumpanija jew istituzzjoni ta' daqs medju. Wieħed jista' jsib sommarju fl-appendiċi.

CSIRT Fittizju

5 Strateġija ġenerali għall-ippjanar u t-twaqqif ta' CSIRT

Għal bidu b'suċċess tal-proċess tat-twaqqif ta' CSIRT huwa importanti li jkun hemm viżjoni ċara tas-servizzi possibbli li t-tim jista' joffri lill-klijenti tiegħu, fid-"dinja tal-CSIRT" magħrufin aħjar bħala 'kostitwenti'. Għalhekk huwa importanti li wieħed jifhem x'inhuma l-ħtiġijiet tal-kostitwenti sabiex jipprovdi servizzi adegwati fil-mument u l-kwalità opportuni.

X'inhu CSIRT?

CSIRT tfisser Tim ta' Rispons għall-Inċidenti ta' Sigurtà tal-Kompjuter. It-terminu CSIRT huwa użat l-aktar fl-Ewropa għat-terminu protett CERT, li huwa rreġistrat fl-USA miċ-Ċentru ta' Koordinament tal-CERT (CERT/CC).
Jeżistu diversi abbrevjazzjonijiet li jintużaw għall-istess xorta ta' timijiet:

- CERT jew CERT/CC (Tim ta' Rispons għall-Emerġenzi tal-Kompjuter / Ċentru ta' Koordinament)
- CSIRT (Tim ta' Rispons għall-Inċidenti ta' Sigurtà tal-Kompjuter)
- IRT (Tim ta' Rispons għall-Inċidenti)
- CIRT (Tim ta' Rispons għall-Inċidenti tal-Kompjuter)
- SERT (Tim ta' Rispons għal Emerġenza tas-Sigurtà)

L-ewwel tfaqqigħ importanti ta' worm fl-infrastruttura globali ta' l-IT seħħ lejn l-aħħar ta' l-1980s. Il-worm issemma Morris[2] u nfirex malajr, biex fil-fatt infetta numru kbir ta' sistemi ta' l-IT madwar id-dinja.

Dan l-inċident serva bħala sejħa ta' qawmien: f'daqqa waħda n-nies indunaw bil-bżonn kbir ta' kooperazzjoni u koordinazzjoni bejn l-amministraturi tas-sistema u l-ġesturi ta' l-IT sabiex jindirizzaw każijiet bħal dan. Minħabba l-fatt li l-ħin kien fattur kritiku, kellu jiġi stabbilit approċċ aktar stabbilit u strutturali għall-immaniġġar ta' inċidenti tas-sigurtà fl-IT. U għalhekk ftit jiem wara l-"inċident Morris", l-Aġenzija dwar Proġetti Avvanzati ta' Riċerka tad-Difiża (DARPA) stabbiliet l-ewwel CSIRT: iċ-Ċentru ta' Koordinament tal-CERT (CERT/CC[3]), li jinsab fil-Carnegie Mellon University f'Pittsburgh (Pennsylvania).

Dan il-mudell malajr ġie adottat fl-Ewropa, u fl-1992 il-fornitur Akkademiku Olandiż SURFnet introduċa l-ewwel CSIRT fl-Ewropa, imsemmi SURFnet-CERT[4]. Wara segwew bosta timijiet u attwalment l-*Inventarju ta' l-attivitajiet CERT fl-Ewropa*[5] ta' l-ENISA jelenka aktar minn 100 tim magħruf li jinsabu fl-Ewropa.

Matul is-snin il-CERTs wessgħu l-kapaċitajiet tagħhom minn sempliċi forza ta' reazzjoni għal forniturі ta' servizzi tas-sigurtà kompleti, li jinkludu servizzi preventivi bħal twissijiet, konsulenzi dwar is-sigurtà, taħriġ u servizzi ta' ġestjoni tas-sigurtà. It-terminu "CERT" malajr ġie kkunsidrat bħala insuffiċjenti. Għalhekk, ġie stabbilit it-terminu ġdid "CSIRT" fl-aħħar ta' l-1990s. Attwalment iż-żewġ termini (CERT u CSIRT) jintużaw bl-istess tifsira, b'CSIRT ikun l-aktar terminu preċiż.

[2] Aktar dwar il-Morris Worm http://en.wikipedia.org/wiki/Morris_worm

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

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

[5] Inventarju ta' ENISA http://www.enisa.europa.eu/cert_inventory/

5..1 It-terminu *Kostitwenza*

Minn issa 'l quddiem it-terminu 'kostitwenza' (fil-komunitajiet CSIRT) li issa jinsab stabbilit sewwa, se jintuża biex jirreferi għall-bażi tal-klijenti ta' CSIRT. Klijent wieħed se jiġi indirizzat bħala 'kostitwent', waqt li grupp ta' klijenti bħala 'kostitwenti'.

5..2 Definizzjoni ta' CSIRT

CSIRT huwa tim ta' esperti tas-sigurtà ta' l-IT li x-xogħol prinċipali tagħhom huwa li jirrispondu għal inċidenti tas-sigurtà tal-kompjuter. Huwa jipprovdi s-servizzi neċessarji biex jiġu indirizzati u jgħinu lill-kostitwenti tagħhom biex jirkupraw minn vjolazzjonijiet.

Sabiex jitnaqqsu r-riskji u jiġi limitat in-numru ta' risponsi meħtieġa, il-biċċa l-kbira tal-CSIRTs jipprovdu wkoll servizzi preventivi u edukattivi għall-kostitwenza tagħhom. Huma joħorġu konsulenzi dwar vulnerabilitajiet fis-softwer u l-ħardwer li jkun qiegħed jintuża, u jinfurmaw ukoll lill-utenti dwar sfruttamenti u vajrusijiet li japprofittaw minn dawn in-nuqqasijiet. Għalhekk il-kostitwenti jistgħu jirranġaw u jaġġornaw malajr is-sistemi tagħhom. Ara kapitlu *5.2 Servizzi possibbli* għal lista sħiħa ta' servizzi possibbli.

5..3 Il-vantaġġi li jkollok CSIRT

Li jkollok tim iddedikat għas-sigurtà ta' l-IT jgħin organizzazzjoni biex tnaqqas u tevita inċidenti importanti u jgħin għall-protezzjoni ta' l-assi prezzjużi tagħha

Aktar benefiċċji possibbli huma:

- Li jkun hemm koordinazzjoni ċentrali għal kwistjonijiet ta' sigurtà ta' l-IT fi ħdan organizzazzjoni (Punt ta' Kuntatt, PoC).
- Immaniġġar u rispons ċentralizzat u speċjalizzat ta' inċidenti ta' l-IT.
- Li jkollok il-kompetenza fil-qrib biex tappoġġja u tgħin lill-utenti jirkupraw malajr minn inċidenti tas-sigurtà.
- Li jieħu ħsieb kwistjonijiet legali u jżomm l-evidenza f'każ ta' taħrika.
- Li jżomm rekord ta' l-iżviluppi fil-qasam tas-sigurtà.
- Li jistimula kooperazzjoni fi ħdan il-kostitwenza dwar is-sigurtà ta' l-IT (tkabbir ta' l-għarfien).

CSIRT fittizju (pass 0)
Fehim ta' x'inhu CSIRT: Il-CSIRT kampjun irid jaqdi istituzzjoni medja magħmula minn 200 membru tal-persunal. L-istituzzjoni għandha d-dipartiment ta' l-IT tagħha stess u żewġ uffiċċji fergħa oħra fl-istess pajjiż. L-IT għandu rwol importanti għall-kumpanija għaliex jintuża għall-komunikazzjoni interna, netwerk ta' informazzjoni u e-kummerċ 24x7. L-istituzzjoni għandha n-netwerk tagħha stess u tiddisponi minn kollegament żejjed ma' l-internet permezz ta' żewġ ISPs differenti.

5..4 Deskrizzjoni tat-tipi differenti ta' ambjenti tal-CSIRT

Għamilna l-ewwel pass 1. Fehim ta' x'inhu CSIRT u x'benefiċċji jista' jipprovdi. >> Il-pass li jmiss huwa li nwieġbu l-mistoqsija: "Għal liema settur ser jitwasslu s-servizzi tal-CSIRT?"

Meta tibda CSIRT (eżatt bħal kull negozju ieħor) huwa importanti ħafna li tibni malajr kemm jista' jkun idea ċara ta' min huma l-kostitwenti u għal liema tip ta' ambjent se jkunu żviluppati s-servizzi tal-CSIRT. Attwalment niddistingwu s-'setturi' li ġejjin, li huma elenkati b'mod alfabetiku:

- CSIRT għas-Settur Akkademiku
- CSIRT Kummerċjali
- CSIRT għas-Settur tal-CIP/CIIP
- CSIRT għas-Settur Governattiv
- CSIRT Intern
- CSIRT għas-Settur Militari
- CSIRT Nazzjonali
- CSIRT għas-Settur ta' l-Intrapriżi Żgħar u Medji (SME)
- CSIRT tal-Bejjiegħ

CSIRT għas-Settur Akkademiku
Konċentrazzjoni
CSIRT għas-settur akkademiku jipprovdi servizzi ta' CSIRT lil istituzzjonijiet akkademiċi u edukattivi, bħal universitajiet jew faċilitajiet tar-riċerka, u l-ambjenti ta' l-Internet fuq il-kampus tagħhom.

Kostitwenti
Il-kostitwenti tipiċi ta' dan it-tip ta' CSIRT huma l-istaff u l-istudenti ta' l-universitajiet.

CSIRT Kummerċjali
Konċentrazzjoni
CSIRT kummerċjali jipprovdi servizzi ta' CSIRT b'mod kummerċjali lill-kostitwenti tagħhom. Fil-każ ta' ISP, il-CSIRT jipprovdi l-aktar servizzi kontra l-abbużi lill-klijenti finali (Dial-in, ADSL) u servizzi ta' CSIRT lill-klijenti professjonali tagħhom.

Kostitwenti
CSIRTs kummerċjali ġeneralment jagħtu s-servizzi tagħhom lil kostitwenti li jħallsu għalihom.

CSIRT għas-Settur tal-CIP/CIIP
Konċentrazzjoni
Il-CSIRTs f'dak is-settur jiffokaw prinċipalment fuq Protezzjoni ta' Informazzjoni Kritika u / jew protezzjoni ta' Informazzjoni u Infrastruttura Kritika. Fil-maġġoranza tal-każijiet dan il-CSIRT speċjalizzat jikkoopera mill-qrib ma' dipartiment Governattiv tal-CIIP. Huwa jkopri s-setturi kritiċi kollha ta' l-IT fil-pajjiż u jipproteġi liċ-ċittadini ta' dak il-pajjiż.

Kostitwenti
Il-Gvern; negozji kritiċi ta' l-IT; iċ-ċittadini

CSIRT għas-Settur Governattiv
Konċentrazzjoni
CSIRT governattiv jipprovdi servizzi lil aġenziji tal-gvern u f'xi pajjiżi liċ-ċittadini.

Kostitwenti
Aġenziji tal-gvern jew relatati mal-gvern; f'xi pajjiżi s-servizzi ta' twissija huma pprovduti wkoll liċ-ċittadini (per eżempju fil-Belġju, l-Ungerija, l-Olanda, ir-Renju Unit jew il-Ġermanja).

CSIRT Intern
Konċentrazzjoni
CSIRT intern jipprovdi servizzi lill-organizzazzjoni li jkun fiha biss. Dan jiddeskrivi aktar il-funzjonament pjuttost milli settur. Ħafna organizzazzjonijiet tat-telekomunikazzjoni u banek per eżempju għandhom il-CSIRTs interni tagħhom stess. Ġeneralment ma jżommux websajt għall-pubbliku.

Kostitwenti
Il-persunal intern u d-dipartiment ta' l-IT ta' l-organizzazzjoni li jkun fiha

CSIRT għas-Settur Militari
Konċentrazzjoni
CSIRT f'dak is-settur jipprovdi servizzi lil organizzazzjonijiet militari b'responsabbiltajiet għal infrastruttura ta' l-IT li hija meħtieġa għal skopijiet ta' difiża.

Constituents
Il-persunal ta' istituzzjonijiet militari jew entitajiet relatati mill-qrib, per eżempju d-Dipartiment tad-Difiża

CSIRT Nazzjonali
Konċentrazzjoni
CSIRT b'konċentrazzjoni nazzjonali, ikkunsidrat bħala punt ta' kuntatt tas-sigurtà għal pajjiż. F'xi każijiet il-CISRT governattiv jaġixxi wkoll bħala PoC nazzjonali (bħall-UNIRAS fir-Renju Unit).

Kostitwenti
Dan it-tip ta' CSIRT ġeneralment ma jkollux kostitwenti diretti, billi l-CSIRT nazzjonali jilgħab biss rwol intermedjarju għall-pajjiż kollu

CSIRT għas-Settur ta' l-Intrapriżi Żgħar u Medji (SME)

Konċentrazzjoni
CSIRT organizzat minnu nnifsu li jipprovdi s-servizzi tiegħu lill-fergħa tan-negozju tiegħu stess jew lil grupp ta' utenti simili.

Kostitwenti
Il-kostitwenti ta' dawn il-CSIRTs jistgħu jkunu SMEs u l-persunal tagħhom, jew gruppi ta' interess speċjali bħall-"Assoċjazzjoni tal-Bliet u l-Muniċipalitajiet" ta' pajjiż.

CSIRT tal-Bejjiegħ
Konċentrazzjoni
CSIRT tal-bejjiegħ jiffoka fuq l-appoġġ tal-prodott speċifiċi għall-bejjiegħ. Il-mira tiegħu ġeneralment hija li jiżviluppa u jipprovdi soluzzjonijiet bil-għan li jitneħħew vulnerabilitajiet u jitnaqqsu l-effetti negattivi potenzjali tad-difetti.

Kostitwenti
Sidien tal-prodott

Kif deskritt fil-paragrafu dwar il-CSIRTs nazzjonali, huwa possibbli li tim jaqdi aktar minn settur wieħed. Dan għandu impatt ngħidu aħna fuq l-analiżi tal-kostitwenza u l-ħtiġijiet tagħha.

CSIRT fittizju (pass 1)
Fażi tal-bidu Fil-fażi tal-bidu l-CSIRT il-ġdid ikun ippjanat bħala CSIRT Intern, li jipprovdi s-servizzi tiegħu lill-kumpanija li tospitah, lid-dipartiment lokali ta' l-IT u lill-persunal. Huwa jsostni u jikkoordina wkoll l-immaniġġar ta' inċidenti relatati mas-sigurtà ta' l-IT bejn l-uffiċċji tal-fergħat differenti.

Servizzi possibbli li jista' jagħti CSIRT

Għamilna l-ewwel żewġ passi

1. Fhimna x'inhu CSIRT u x'benefiċċji jista' jipprovdi.
2. Lil liema settur ser jipprovdi s-servizzi tiegħu t-tim il-ġdid?

>> Il-pass li jmiss huwa li titwieġeb il-mistoqsija, *x'servizzi għandhom jiġu pprovduti lill-kostitwenti*.

Hemm bosta servizzi li CSIRT jista' jagħti, iżda sa issa l-ebda CSIRT eżistenti ma jipprovdihom kollha. Għalhekk l-għażla tas-sett xieraq ta' servizzi hija deċiżjoni importanti ħafna. Taħt għandek issib ħarsa ġenerali qasira tas-servizzi kollha magħrufa ta' CSIRT, kif definiti fil-"Manwal għall-CSIRTs" ippubblikat mill-CERT/CC[6].

[6] CERT/CC Manwal għall-CSIRTs http://www.cert.org/archive/pdf/csirt-handbook.pdf

Servizzi Reattivi	**Servizzi Proattivi**	**Immaniġġar ta' l-Artefatt**
• **Allarmi u Twissijiet** • **Immaniġġar ta' Inċident** • **Analiżi ta' Inċident** • **Appoġġ b'Rispons għal Inċident** • **Koordinament tar-Rispons għal Inċident** • Rispons għall-Inċident fuq il-post • Immaniġġar tal-Vulnerabilità • Analiżi tal-Vulnerabilità • Rispons għall-vulnerabilità • Koordinament tar-rispons għall-vulnerabilità	• **Dikjarazzjonijiet** • Għassa għat-Teknoloġija • Verifiki u Evalwazzjonijiet tas-Sigurtà • Konfigurazzjoni u Manutenzjoni tas-Sigurtà • Żvilupp ta' Għodod tas-Sigurtà • Servizzi għas-Sejbien ta' Intrużjoni • Tixrid ta' Informazzjoni Relatata mas-Sigurtà	• *Analiżi ta' l-artefatt* • *Rispons għall-artefatt* • *Koordinament tar-rispons għall-artefatt* ***Ġestjoni tal-Kwalità tas-Sigurtà*** • *Analiżi tar-Riskju* • *Kontinwità tan-Negozju u Irkupru minn Diżastru* • *Konsulenza dwar is-Sigurtà* • *Tkabbir ta' l-Għarfien* • *Edukazzjoni/Taħriġ* • *Evalwazzjoni jew Ċertifikazzjoni tal-Prodott*

Fig. 1 Lista ta' Servizzi ta' CSIRT mill-CERT/CC[7]

Is-servizzi prinċipali (immarkati b'ittri grassi): saret distinzjoni bejn servizzi reattivi u servizzi proattivi. Is-servizzi proattivi huma mmirati lejn il-prevenzjoni ta' l-inċidenti permezz ta' tkabbir ta' l-għarfien u t-taħriġ, filwaqt li s-servizzi reattivi huma mmirati lejn il-ġestjoni ta' l-inċidenti u t-tnaqqis tad-dannu li jirriżulta.

Immaniġġar ta' l-artefatt jinkludi l-analiżi ta' kwalunkwe fajl jew oġġett misjub fuq sistema li jista' jkun involut f'azzjonijiet ħżiena, bħal fdalijiet minn virus, *worms*, *scripts*, *trojans*, eċċ. Jinkludi wkoll l-immaniġġar u t-tqassim ta' l-informazzjoni li tirriżulta lill-bejjiegħa u partijiet oħra interessati, sabiex jiġi evitat aktar tixrid ta' softwer malizzjuż u biex jitnaqqsu r-riskji.

Is-Servizzi ta' Sigurtà u ta' Ġestjoni tal-Kwalità huma servizzi b'miri aktar fit-tul u jinkludu konsulenza u miżuri edukattivi.

Ara l-appendiċi għal spjegazzjoni dettaljata tas-servizzi ta' CSIRT.

Li tagħżel is-servizzi korretti għall-kostitwenti tiegħek huwa pass importanti u se ssir aktar referenza għalih fil-kapitlu *6.1 Definizzjoni tal-Mudell Finanzjarju*.

Il-biċċa l-kbira tal-CSIRTS jibdew billi jqassmu 'Allarmi u Twissijiet', jagħmlu 'Dikjarazzjonijiet' u jipprovdu 'Immaniġġar ta' l-Inċident' għall-kostitwenti tagħhom. Dawn is-servizzi prinċipali ġeneralment jagħtu profil tajjeb u valur ta' l-attenzjoni mal-kostitwenza, u huma kkunsidrati l-aktar bħala "valur miżjud" reali.

[7] Lista ta' Servizzi ta' CSIRT mill-CERT/CC: http://www.cert.org/csirts/services.html

Metodu tajjeb huwa li tibda bi grupp żgħir ta' kostitwenti-pilota, tagħti s-servizzi prinċipali għal perjodu-pilota ta' żmien u titlob kummenti wara.
L-utenti-pilota interessati ġeneralment jipprovdu kummenti kostruttivi u jgħinu biex jiġu żviluppati servizzi skond il-ħtiġijiet ta' l-utent.

CSIRT fittizju (pass 2)
Għażla tas-servizzi korretti
Fil-fażi tal-bidu ġie deċiż li l-CSIRT il-ġdid jiffoka prinċipalment fuq li jipprovdi xi wħud mis-servizzi ċentrali għall-impjegati.

Ġie deċiż li wara fażi-pilota tista' tiġi kkunsidrata l-estensjoni tal-portafoll ta' servizzi u jistgħu jiżdiedu xi 'Servizzi ta' Ġestjoni tas-Sigurtà". Dik id-deċiżjoni ssir fuq il-bażi tal-kummenti mill-kostitwenti-pilota u f'kollaborazzjoni mill-qrib mad-dipartiment għall-Assigurazzjoni tal-Kwalità.

Analiżi tal-kostitwenza u dikjarazzjoni tal-missjoni

Għamilna l-ewwel tliet passi:

1. Fhimna x'inhu CSIRT u x'benefiċċji jista' jipprovdi.
2. Lil liema settur ser jagħti s-servizzi tiegħu t-tim il-ġdid?
3. X'tipi ta' servizzi jista' jipprovdi CSIRT lill-kostitwenza tiegħu.

>> Il-pass li jmiss huwa li titwieġeb il-mistoqsija, *x'tip ta' approċċ għandu jintgħażel biex jinbeda CSIRT?*

Il-pass li jmiss huwa ħarsa aktar fil-fond lejn il-kostitwenza bl-objettiv prinċipali li jintgħażlu l-kanali korretti ta' komunikazzjoni:

- Jiġi mfisser l-approċċ tal-komunikazzjoni lill-kostitwenti
- Tiġi definita d-dikjarazzjoni tal-missjoni
- Isiru implimentazzjoni/pjan tal-proġett realistiċi
- Jiġu definiti s-servizzi tal-CSIRT
- Tiġi definita l-istruttura organizzattiva
- Tiġi definita l-politika dwar is-Sigurtà ta' l-Informazzjoni
- Jiġi mħaddem il-persunal korrett
- Użu ta' l-uffiċċju tal-CSIRT tiegħek
- Tfittxija għal kooperazzjoni bejn CSIRTs oħra u inizjattivi nazzjonali possibbli

Dawn il-passi ser jiġu deskritti aktar fid-dettall fil-paragrafi li ġejjin u jistgħu jintużaw bħala input għall-pjan korporattiv u tal-proġett.

5..1 Approċċ ta' komunikazzjoni għall-kostitwenza

Kif intqal qabel, huwa importanti ħafna li tkun taf il-ħtiġijiet tal-kostitwenza kif ukoll l-istrateġija tiegħek ta' komunikazzjoni, fosthom il-kanali ta' komunikazzjoni li huma l-aktar adattati biex tavviċinahom bl-informazzjoni.

It-teorija ta' l-immaniġġar taf diversi approċċi possibbli għal din il-problema li jiġi analizzat grupp fil-mira. F'dan id-dokument niddeskrivi tnejn minnhom: l-analiżi SWOT u l-analiżi PEST.

Analiżi SWOT
Analiżi SWOT hija għodda strateġika ta' l-ippjanar użata biex jiġu evalwati s-**S**aħħiet, id-Dgħjufijiet (**W**eaknesses), l-**O**pportunitajiet, u t-**T**heddidiet involuti fi proġett jew f'impriża kummerċjali jew fi kwalunkwe sitwazzjoni oħra li teħtieġ deċiżjoni. Din it-teknika hija attribwita lil Albert Humphrey, li mexxa proġett ta' riċerka fl-Università ta' Stanford fl-1960s u 1970s, billi uża dejta mill-kumpaniji ta' Fortune 500.[8]

Saħħa	**Dgħjufija**
Opportunitajiet	**Theddidiet**

Fig. 2 Analiżi SWOT

[8] Analiżi SWOT fil-Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Analiżi PEST

L-analiżi PEST hija għodda oħra importanti u użata b'mod estensiv biex tiġi analizzata l-kostitwenza bil-għan li jkunu mifhuma ċ-ċirkustanzi **P**olitiċi, **E**konomiċi, **S**oċjo-kulturali u **T**eknoloġiċi ta' l-ambjent li jkun qed jopera fih CSIRT. Hija tgħin biex jiġi stabbilit jekk l-ippjanar ikunx għadu jaqbel ma' l-ambjent u probabbli tgħin biex jiġu evitati azzjonijiet meħuda minn ipoteżi ħżiena.

Politiċi	**Ekonomiċi**
• Kwistjonijiet ekoloġiċi/ambjentali • Is-suq domestiku tal-leġislazzjoni attwali • Leġislazzjoni futura • Leġislazzjoni Ewropea/internazzjonali • Organi u proċessi regolatorji • Politika tal-gvern • Mandat u bidla tal-gvern • Politika kummerċjali • Fondi, għotjiet u inizjattivi • Gruppi ta' lobbying/pressjoni lokali • Gruppi ta' pressjoni internazzjonali	• Sitwazzjoni ekonomika lokali • Xejriet ekonomiċi lokali • Ekonomiji u xejriet barranin • Kwistjonijiet ġenerali ta' tassazzjoni • Tassazzjoni speċifika għall-prodott/servizzi • Kwistjonijiet staġjonali/tat-temp • Ċikli tas-suq u kummerċjali • Fatturi speċifiċi ta' l-industrija • Rotot tas-suq u xejriet tad-distribuzzjoni • Motivaturi tal-klijent/utent finali • Rati ta' l-interess u tal-kambju
Soċjali	**Teknoloġiċi**
• Xejriet fl-istil ta' ħajja • Demografiċi • Attitudnijiet u opinjonijiet tal-konsumatur • Opinjonijiet tal-medja • Bidliet fil-liġi li jaffettwaw fatturi soċjali • Immaġni tal-marka, tal-kumpanija, tat-teknoloġija • Mudelli tax-xiri tal-konsumatur • Moda u mudelli tar-rwol • Avvenimenti u influwenzi importanti • Aċċess u xejriet tax-xiri • Fatturi etniċi/reliġjuži • Riklami u pubbliċità	• Żviluppi kompettitivi fit-teknoloġija • Finanzjament tar-riċerka • Teknoloġiji relatati/dipendenti • Teknoloġija/soluzzjonijiet ta' sostituzzjoni • Maturazzjoni tat-teknoloġija • Maturazzjoni u kapaċità tal-manifattura • Informazzjoni u komunikazzjoni • Mekkaniżmi/teknoloġija tax-xiri tal-konsumatur • Leġislazzjoni teknoloġika • Potenzjal ta' l-innovazzjoni • Aċċess għat-teknoloġija, liċenzjar, patenti • Kwistjonijiet ta' proprjetà intellettwali

Fig. 3 Mudell ta' Analiżi PEST

Deskrizzjoni dettaljata ta' l-analiżi PEST tista' tinstab fil-Wikipedia[9].

Iż-żewġ għodod jagħtu ħarsa ġenerali komprensiva u strutturata ta' x'inhuma l-ħtiġijiet tal-kostitwenti. Ir-riżultati jikkumplimentaw il-proposta tan-negozju u b'din l-għajnuna biex jinkiseb l-iffinanzjar għat-twaqqif tal-CSIRT.

Kanali ta' komunikazzjoni

Suġġett importanti li għandu jiġi inkluż fl-analiżi huma metodi possibbli ta' komunikazzjoni u ta' tqassim ta' l-informazzjoni ("Kif tikkomunika mal-kostitwenza?")

Jekk ikun possibbli, żjarat personali regolari tal-kostitwenti għandhom jiġu kkunsidrati. Huwa fatt magħruf li l-laqgħat wiċċ imb'wiċċ iħaffu l-kollaborazzjoni. Jekk iż-żewġ naħat huma lesti li jaħdmu flimkien, dawn il-laqgħat iwasslu għal relazzjoni aktar miftuħa.

[9] Analiżi PEST fil-Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Ġeneralment il-CSIRTs jużaw sett ta' kanali tal-komunikazzjoni. Dawn li ġejjin irriżultaw utli fil-prattika u ta' min jikkunsidrahom

- Websajt pubblika
- Żona magħluqa tal-membri fuq il-websajt
- Formoli tal-web biex jiġu rrappurtati inċidenti
- Listi ta' l-impustar (mailing lists)
- E-mail personalizzat
- Telefon / Faks
- SMS
- Ittri 'konvenzjonali' fuq karta
- Rapporti kull xahar jew annwali

Minbarra li jużaw e-mail, formoli tal-web, telefon jew faks biex jiffaċilitaw l-immaniġġar ta' inċident (biex jirċievu rapporti ta' l-inċident mill-kostitwenza, jikkoordinaw ma' timijiet oħra jew jagħtu kummenti u appoġġ lill-vittma), bosta CSIRTs jippubblikaw il-pariri tagħhom dwar is-sigurtà fuq websajt miftuħa għall-pubbliku jew permezz ta' listi ta' l-impustar.

! Jekk ikun possibbli, l-informazzjoni għandha tiġi distribwita b'mod sigur. L-emails ngħidu aħna jistgħu jiġu ffirmati b'mod diġitali b'PGP, u informazzjoni sensittiva dwar inċidenti għandha dejjem tintbagħat kodifikata.

Għal aktar informazzjoni ara l-kapitlu *8.5 Għodod disponibbli ta' CSIRT*. Ara wkoll kapitlu 2.3 tar-*RFC2350*[10].

CSIRT fittizju (pass 3a)

Issir analiżi tal-kostitwenza u tal-kanali xierqa ta' komunikazzjoni

Sessjoni ta' brainstorming ma' wħud mill-persuni prinċipali ta' l-amministrazzjoni u l-kostitwenza ġġenerat biżżejjed input għal analiżi SWOT. Din wasslet għall-konklużjoni li hemm ħtieġa għas-servizzi prinċipali:

- Allarmi u twissijiet
- Ġestjoni ta' l-inċident (analiżi, appoġġ tar-rispons u koordinament tar-rispons)
- Dikjarazzjonijiet

Irid jiġi assigurat li l-informazzjoni tiġi distribwita b'mod organizzat biex tilħaq l-akbar parti possibbli tal-kostitwenza. Għalhekk ittieħdet id-deċiżjoni li allarmi, twissijiet u avviżi fil-forma ta' dikjarazzjonijiet dwar is-sigurtà jiġu ppubblikati fuq websajt iddedikata u mqassma permezz ta' lista ta' l-impustar. Il-CSIRT jiffaċilita l-email, it-telefon u l-faks biex jirċievi rapporti ta' l-inċidenti. Hija ppjanata formola tal-web integrata għall-pass li jmiss.

Ara l-paġna li jmiss għal eżempju ta' analiżi SWOT.

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

Saħħa • Hemm xi għarfien fi ħdan il-kumpanija • Jogħġobhom il-pjan u lesti biex jikkooperaw • Appoġġ u finanzjament mill-bord tat-tmexxija	**Dgħjufija** • M'hemmx wisq komunikazzjoni bejn id-dipartimenti differenti u l-uffiċċji tal-fergħat. • Ebda koordinazzjoni fl-inċidenti ta' l-IT • Ħafna "dipartimenti żgħar"
Opportunitajiet • Fluss kbir ta' informazzjoni mhux strutturata dwar il-vulnerabilità • Bżonn qawwi għal koordinazzjoni • Tnaqqis tat-telf minħabba l-inċidenti • Ħafna truf miftuħin dwar il-kwistjoni tas-sigurtà ta' l-IT • Il-persunal jiġi edukat dwar is-sigurtà ta' l-IT	**Theddidiet** • M'hemmx wisq flus disponibbli • M'hemmx wisq ħaddiema • Aspettattivi għoljin • Il-kultura

Fig. 4 Eżempju ta' analiżi SWOT

5..2 Dikjarazzjoni tal-missjoni

Wara li jiġu analizzati l-ħtiġijiet u x-xewqat tal-kostitwenza rigward is-servizzi tal-CSIRT, il-pass li jmiss għandu jkun it-tfassil ta' dikjarazzjoni tal-missjoni.

Dikjarazzjoni tal-missjoni tiddeskrivi l-funzjoni bażika ta' l-organizzazzjoni fis-soċjetà, f'termini tal-prodotti u s-servizzi li tipprovdi lill-kostitwenti tagħha. Hija tippermetti li titwassal b'mod ċar l-eżistenza u l-funzjoni tal-CSIRT il-ġdid.

Hija prattika tajba li tagħmel id-dikjarazzjoni tal-missjoni kompatta iżda mhux riġida żżejjed, għaliex ġeneralment din tibqa' l-istess għal numru ta' snin.

Dawn li ġejjin huma xi eżempji ta' stqarrijiet tal-missjoni minn CSIRTs operattivi:

"<Isem tal-CSIRT> jipprovdi tagħrif u assistenza lill-<kostitwenti tiegħu (iddefinixxi l-kostitwenti tiegħek)> fl-implimentazzjoni ta' miżuri proattivi biex jitnaqqsu r-riskji ta' inċidenti ta' sigurtà tal-kompjuter kif ukoll jirrispondi għal tali inċidenti meta jseħħu."

"Biex joffri appoġġ lill-<Kostitwenti> fuq il-prevenzjoni u r-rispons għal Inċidenti ta' Sigurtà relatati ma' l-IT"[11]

[11] Dikjarazzjoni tal-missjoni ta' Govcert.nl: http://www.govcert.nl

Id-dikjarazzjoni tal-missjoni hija pass importanti ħafna u neċessarju biex tibda. Jekk jogħġbok irreferi għall-kapitlu *2.1* tar-*RFC2350*[12] għal deskrizzjoni aktar dettaljata ta' l-informazzjoni li CSIRT għandu jippubblika.

CSIRT fittizju (pass 3b)
Il-maniġment tal-CSIRT fittizju għamel id-dikjarazzjoni tal-missjoni segwenti: *"CSIRT Fittizju jipprovdi tagħrif u assistenza lill-persunal tal-kumpanija li tospitah biex inaqqas ir-riskji ta' inċidenti ta' sigurtà fil-kompjuters kif ukoll jirrispondi għal tali inċidenti meta jseħħu."* B'din, il-CSIRT fittizju jagħmilha ċara li huwa CSIRT intern u li x-xogħol prinċipali tiegħu huwa li jieħu ħsieb kwistjonijiet relatati mas-sigurtà ta' l-IT.

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

6 Żvilupp tal-Pjan Korporattiv

Għamilna l-passi li ġejjin:

1. Fhimna x'inhu CSIRT u x'benefiċċji jista' jipprovdi.
2. Lil liema settur ser jipprovdi s-servizzi tiegħu t-tim il-ġdid?
3. X'tipi ta' servizzi CSIRT jista' jipprovdi lill-kostitwenza tiegħu.
4. Analiżi ta' l-ambjent u l-kostitwenza
5. Definizzjoni tad-dikjarazzjoni tal-missjoni

>> Il-pass li jmiss huwa li jiġi definit il-pjan tan-negozju

Ir-riżultat mill-analiżi jagħtik ħarsa ġenerali tajba tal-ħtiġijiet u d-dgħjufijiet (preżunti) tal-kostitwenza, għalhekk huwa meħud bħala input għall-pass li jmiss.

Definizzjoni tal-mudell finanzjarju

Wara l-analiżi ġew magħżula ftit servizzi prinċipali biex wieħed jibda. Il-pass li jmiss huwa li wieħed jaħseb dwar il-mudell finanzjarju: x'parametri ta' għoti tas-servizz huma kemm adattati kif ukoll jistgħu jitħallsu.

F'dinja perfetta l-finanzjament ikun adattat skond il-ħtiġijiet tal-kostitwenza, iżda fir-realtà l-portafoll ta' servizzi li jistgħu jiġu pprovduti jridu jadattaw għal baġit partikolari. Għalhekk huwa aktar realistiku li wieħed jibda bl-ippjanar tal-kwistjonijiet monetarji.

6..1 Il-mudell ta' l-ispiża

Iż-żewġ fatturi prinċipali li jinfluwenzaw l-ispiża huma l-għażla tal-ħinijiet tas-servizz u n-numru (u l-kwalità) tal-ħaddiema li jridu jiġu impjegati. Hemm bżonn li jiġi pprovdut rispons għall-inċidenti u appoġġ tekniku erbgħa u għoxrin siegħa kuljum jew dawn is-servizzi se jingħataw biss waqt il-ħinijiet tax-xogħol?

Jiddependi mid-disponibilità mixtieqa u t-tagħmir ta' l-uffiċċju (per eżempju huwa possibbli li taħdem mid-dar?), jista' jkun utli li taħdem b'roster tax-xogħol ta' stennija jew roster tax-xogħol ippjanata.

Xenarju immaġinabbli huwa li jingħataw kemm servizzi proattivi kif ukoll servizzi reattivi waqt il-ħinijiet tax-xogħol. Barra l-ħinijiet tax-xogħol jiġu pprovduti biss servizzi limitati, per eżempju fil-każ ta' diżastri u inċidenti kbar biss, minn membru tal-persunal li jkun disponibbli.

Għażla oħra hija li wieħed ifittex kooperazzjoni internazzjonali bejn timijiet CSIRT oħra. Diġà hemm eżempji ta' kooperazzjoni "Following the Sun" li qiegħda tiffunzjona. Ngħidu aħna l-kooperazzjoni bejn timijiet Ewropej u Amerikani ntweriet li hija siewja u tipprovdi mezz tajjeb biex tiġi maqsuma l-kapaċità ta' xulxin. Per eżempju, Sun Microsystems CSIRT, li għandhom diversi fergħat f'żoni tal-ħin differenti madwar id-dinja (iżda huma

lkoll membri ta' l-istess tim CSIRT) jipprovdu servizzi 24x7 billi kontinwament iċaqilqu l-kompiti bejn it-timijiet madwar il-globu. Dan fil-fatt inaqqas l-ispejjeż, billi t-timijiet dejjem jaħdmu biss waqt il-ħinijiet normali tax-xogħol u jipprovdu wkoll servizzi lill-"parti rieqda" tad-dinja.

Hija prassi tajba li tanalizza b'mod partikolari l-ħtieġa għal servizzi 24x7 fil-fond mal-kostitwenza. Allarmi u twissijiet ipprovduti matul il-lejl ma tantx jagħmlu sens meta r-reċipjent se jaqrahom biss l-għada filgħodu. Hemm linja fina bejn li "għandek bżonn servizz" u li "trid servizz", iżda b'mod speċjali l-ħinijiet tax-xogħol jagħmlu differenza enormi fl-għadd ta' ħaddiema u l-faċilitajiet meħtieġa, u għalhekk għandhom impatt importanti ħafna fuq il-mudell ta' l-ispiża.

6..2 Il-mudell tad-dħul

Meta tkun taf l-ispiża huwa pass tajjeb li taħseb dwar mudelli possibbli ta' dħul: kif is-servizzi ppjanati jistgħu jiġu ffinanzjati. Dawn huma xi xenarji possibbli biex jiġu evalwati:

Użu ta' riżorsi eżistenti
Huwa dejjem utli li tevalwa r-riżorsi li diġà jeżistu f'partijiet oħra tal-kumpanija. Diġà hemm personal xieraq impjegat (per eżempju fid-dipartiment ta' l-IT eżistenti) bl-isfond u l-kompetenza meħtieġa? Probabbli jistgħu jinstabu arranġamenti mal-maniġment biex dan il-persunal jiġi ssekondat lill-CSIRT għall-fażi tal-bidu, jew jipprovdu appoġġ għall-CSIRT fuq bażi *ad-hoc*.

Miżata tas-sħubija
Possibilità oħra hija li tbigħ is-servizzi tiegħek lill-kostitwenza, permezz ta' miżata tas-sħubija annwali/kull tliet xhur. Servizzi oħra jistgħu jiġu mħallsa meta jintużaw, per eżempju servizzi ta' konsulenza jew verifiki tas-sigurtà.

Xenarju ieħor immaġinabbli: is-servizzi għall-kostitwenza (interna) jiġu pprovduti mingħajr ħlas, iżda s-servizzi mogħtija lil klijenti esterni jridu jiġu mħallsa. Idea oħra hija li jiġu ppubblikati pariri u bullettini ta' informazzjoni fuq il-websajt pubblika u jkun hemm sezzjoni għall-"Membri Biss" b'informazzjoni speċjali, aktar dettaljata jew imfassla skond il-ħtiġijiet ta' l-utent.

Ġie ppruvat fil-prattika li "Abbonament għal kull servizz ta' CSIRT" għandu biss użu limitat biex jipprovdi biżżejjed fondi, speċjalment fil-fażi tal-bidu. Per eżempju hemm spejjeż bażiċi fissi għat-tim u t-tagħmir li jrid jitħallsu bil-quddiem. L-iffinanzjar ta' dawn l-ispejjeż bil-bejgħ ta' servizzi tal-CSIRT huwa diffiċli u jeħtieġ analiżi finanzjarja dettaljata ħafna biex jinstab il-"punt ta' bilanċ".

Sussidju
Possibbiltà oħra li ta' min jikkunsidraha tista' tkun li wieħed japplika għal sussidju pprovdut mill-gvern jew minn organu governattiv għall-proġett, billi llum bosta pajjiżi għandhom fondi disponibbli għal proġetti ta' sigurtà ta' l-IT. Li tikkuntattja lill-Ministeru ta' l-Intern jista' jkun bidu tajjeb.

Taħlita ta' mudelli ta' xenarju differenti hija naturalment possibbli.

Definizzjoni ta' l-istruttura organizzattiva

L-istruttura organizzattiva xierqa ta' CSIRT tiddependi ħafna fuq l-istruttura eżistenti ta' l-organizzazzjoni li jkun fiha u l-kostitwenza. Tiddependi wkoll fuq l-aċċessibilità ta' esperti mħarrġa li jridu jiġu mħaddma b'mod permanenti jew fuq bażi *ad-hoc*.

CSIRT tipiku jiddefinixxi r-rwoli li ġejjin fi ħdan it-tim:

Ġenerali
- Maniġer ġenerali

Persunal
- Maniġer ta' l-uffiċċju
- Akkawntant
- Konsulent għall-komunikazzjoni
- Konsulent legali

Tim tekniku operattiv
- Mexxej tat-tim tekniku
- Teknixins tekniċi tal-CSIRT, li jagħtu s-servizzi tal-CSIRT
- Riċerkaturi

Konsulenti esterni
- Imqabbda meta meħtieġa

Huwa utli ħafna li jkun hemm espert legali fit-tim speċjalment matul il-fażi tal-bidu tal-CSIRT. Dan se jżid l-ispiża iżda finalment se jiffranka l-ħin u l-problemi legali.

Jiddependi fuq il-varjetà ta' kompetenza fi ħdan il-kostitwenza, u anki meta l-CSIRT ikollu profil għoli mal-medja, irriżulta utli ħafna li jkun hemm ukoll espert tal-komunikazzjoni fit-tim. Dawn l-esperti jistgħu jiffukaw biex jaqilbu kwistjonijiet tekniċi diffiċli f'messaġġi aktar jiftiehmu għall-kostitwenti jew għall-imsieħba tal-medja. L-espert tal-komunikazzjoni jipprovdi wkoll kummenti mill-kostitwenza lill-esperti tekniċi, għalhekk huwa/hija jistgħu jaġixxu bħala "traduttur" u "faċilitatur" bejn dawn iż-żewġ gruppi.

Dawn li ġejjin huma ftit eżempji ta' mudelli organizzattivi użati minn CSIRTs operattivi.

6..1 Il-mudell tan-negozju indipendenti

Il-CSIRT huwa mifrux u jaġixxi bħala organizzazzjoni indipendenti, bit-tmexxija u l-impjegati tiegħu stess.

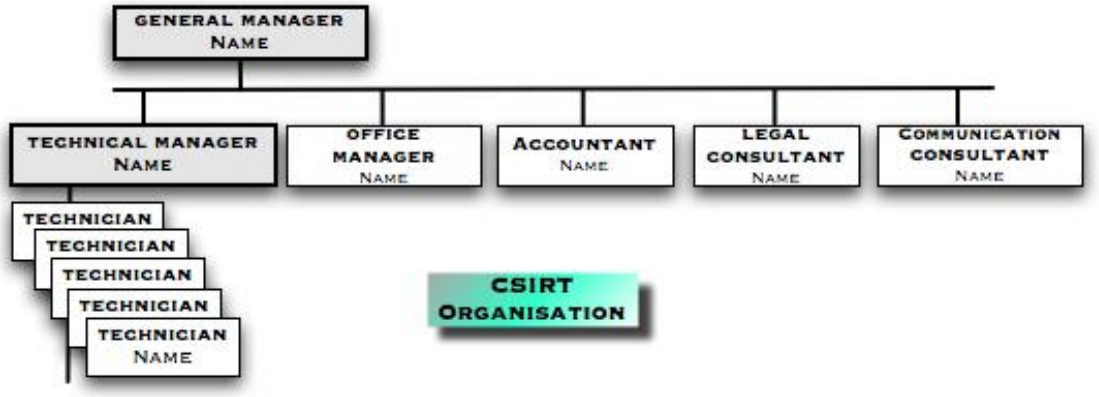


Fig. 5 Mudell ta' Negozju Indipendenti

6..2 Il-mudell inkorporat

Dan il-mudell jista' jintuża jekk CSIRT se jiġi stabbilit f'organizzazzjoni eżistenti, billi per eżempju jintuża dipartiment ta' l-IT eżistenti. Il-CSIRT huwa ggwidat minn mexxej tat-tim li huwa jew hija responsabbli għall-attivitajiet tal-CSIRT. Il-mexxej tat-tim jiġbor it-teknixins neċessarji meta jiġu solvuti inċidenti jew issir ħidma fuq attivitajiet tal-CSIRT. Huwa jew hija jistgħu jitolbu assistenza fi ħdan l-organizzazzjoni eżistenti għal appoġġ speċjalizzat.

Dan il-mudell jista' jiġi adattat ukoll għal sitwazzjonijiet speċifiċi hekk kif jinqalgħu. F'dan il-każ, it-tim ikollu numru fiss jew Ekwivalenti ta' Full Time (FTE) allokat. Il-bank ta' l-abbużi għand ISP, per eżempju, huwa ċertament impjieg *fulltime* għal FTE wieħed jew (fil-maġġoranza tal-każijiet) aktar minn FTE wieħed.

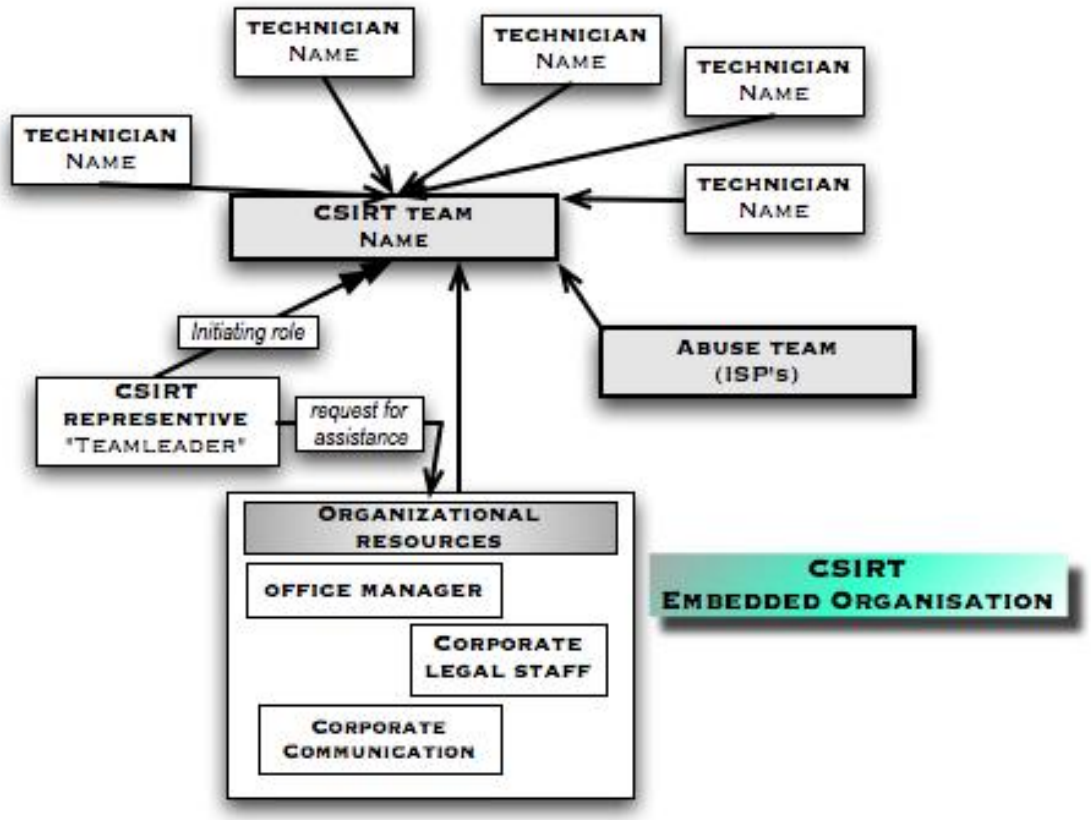


Fig. 6 Mudell organizzattiv inkorporat

6..3 Il-mudell tal-kampus

Kif jissuġġerixxi l-isem, il-mudell tal-kampus huwa adottat primarjament minn CSIRTs akkademiċi u tar-riċerka. Bosta organizzazzjonijiet akkademiċi u tar-riċerka jinkludu diversi universitajiet u faċilitajiet tal-kampus f'postijiet differenti, imxerrda fuq reġjun jew saħansitra fuq il-pajjiż kollu (bħal fil-każ tan-NRENs, in-Netwerks Nazzjonali tar-Riċerka). Ġeneralment dawn l-organizzazzjonijiet huma indipendenti minn xulxin, u ħafna drabi jkollhom il-CSIRT tagħhom stess. Dawn il-CSIRTs ġeneralment ikunu organizzati taħt il-kappa tal-CSIRT 'mamma' jew ċentrali. Il-CSIRT ċentrali jikkoordina u huwa l-punt ta' kuntatt waħdieni għad-dinja ta' barra. Ħafna drabi l-CSIRT ċentrali jipprovdi wkoll is-servizzi prinċipali ta' CSIRT kif ukoll iqassam informazzjoni dwar l-inċident lill-CSIRT tal-kampus rilevanti.

Xi CSIRTs jiċċirkolaw is-servizzi prinċipali tagħhom ta' CSIRT mal-CSIRTs tal-kampus l-oħrajn, li jirriżulta fi spejjeż ġenerali aktar baxxi għall-CSIRT Ċentrali.

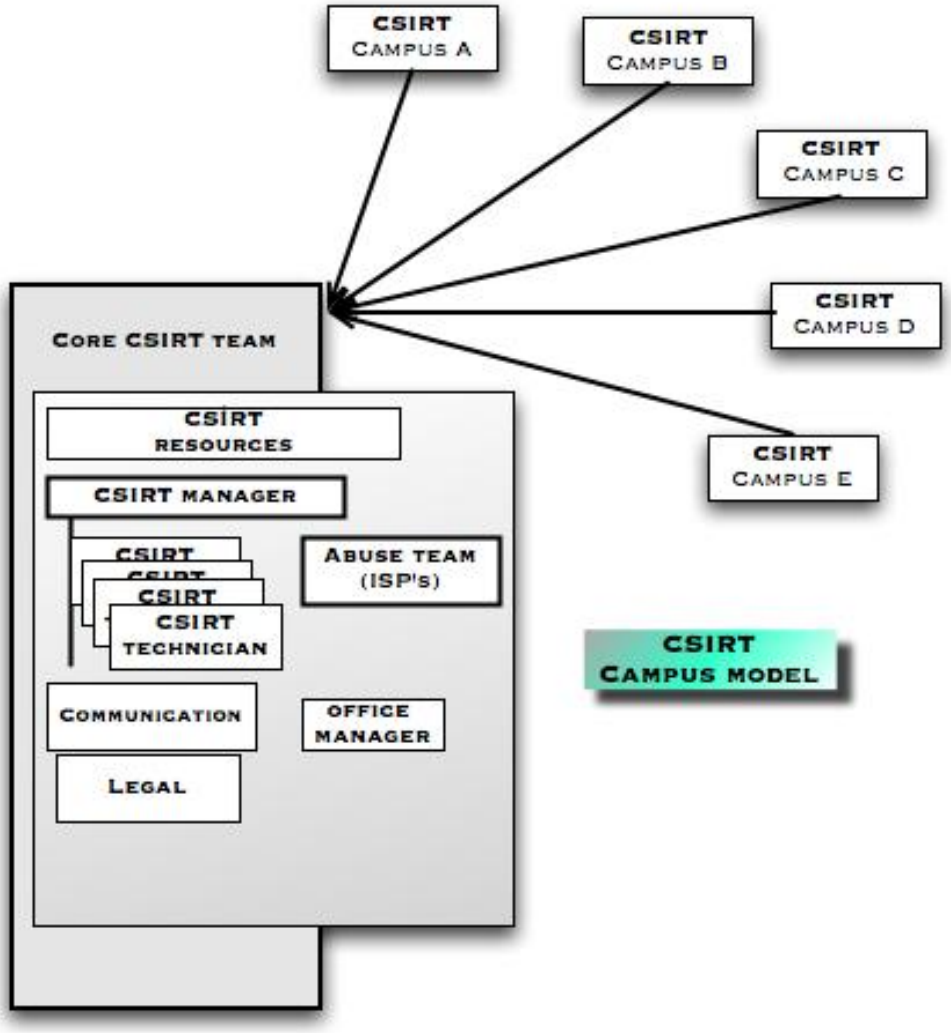


Fig. 7 Il-mudell tal-kampus

6..4 Il-mudell volontarju

Dan il-mudell organizzattiv jiddeskrivi grupp ta' persuni (speċjalisti) li jingħaqdu flimkien biex jipprovdu parir u appoġġ lil xulxin (u lil oħrajn) fuq bażi volontarja. Hija komunità stabbilita b'mod laxk u tiddependi ħafna fuq il-motivazzjoni tal-parteċipanti.

Dan il-mudell huwa per eżempju adottat mill-komunità WARP[13].

Reklutaġġ tal-personal adattat

Wara li jiġu deċiżi s-servizzi u l-livell ta' appoġġ li se jingħata, u wara li jiġi magħżul mudell organizzattiv, il-pass li jmiss huwa li jinstab l-ammont korrett ta' persuni mħarrġa għax-xogħol.

Huwa kważi impossibbli tipprovdi ċifri fattwali dwar l-ammont ta' personal tekniku meħtieġ minn dan il-lat, iżda l-valuri bażiċi li ġejjin ġew ippruvati li huma approċċ tajjeb:

- Sabiex jiġu pprovduti żewġ servizzi prinċipali tat-tqassim ta' bullettini ta' pariri kif ukoll immaniġġar ta' l-inċidenti: minimu ta' **4** FTE.
- Għal servizz sħiħ ta' CSIRT waqt il-ħinijiet tax-xogħol, u żamma tas-sistemi: minimu ta' **6 sa 8** FTE.
- Għal xift 24x7 bil-ħaddiema kollha (żewġ xiftijiet barra l-ħinijiet tax-xogħol), il-minimu huwa **12**-il FTE.

Dawn in-numri jinkludu wkoll ħaddiema żejda għal każijiet ta' mard, vaganzi, eċċ. Huwa wkoll neċessarju li jiġu ċċekkjati l-ftehimiet kollettivi lokali dwar ix-xogħol. Jekk persuni jaħdmu barra l-ħinijiet tax-xogħol, dan jista' jirriżulta fi spejjeż żejda fil-forma ta' allowance li jrid jitħallas.

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

Din li ġejja hija ħarsa ġenerali qasira tal-kompetenzi bażiċi għall-esperti tekniċi ta' CSIRT

Affarijiet ġenerali mid-deskrizzjoni tax-xogħol tal-persunal tekniku:

Kompetenzi personali

- Flessibbli, kreattiv u spirtu tajjeb ta' tim
- Ħiliet analitiċi b'saħħithom
- Kapaċità li tispjega kwistjonijiet tekniċi diffiċli fi kliem sempliċi
- Sensibilità tajba għall-kunfidenzjalità u ħidma b'mod proċedurali
- Ħiliet organizzattivi tajba
- Tiflaħ għall-istress
- Ħiliet komunikattivi u tal-kitba tajbin
- Moħħ miftuħ u rieda li titgħallem

Kompetenzi tekniċi

- Għarfien wiesa' tat-teknoloġija u l-protokolli ta' l-internet
- Għarfien tas-sistemi Linux u Unix (jiddependi fuq it-tagħmir tal-kostitwenza)
- Għarfien tas-sistemi Windows (jiddependi fuq it-tagħmir tal-kostitwenza)
- Għarfien tat-tagħmir ta' l-infrastruttura tan-netwerk (Router, switches, DNS, Proxy, Mail, eċċ.)
- Għarfien ta' l-applikazzjonijiet ta' l-Internet (SMTP, HTTP(s), FTP, telnet, SSH, eċċ.)
- Għarfien tat-theddidiet għas-Sigurtà (DDoS, Phishing, Defacing, sniffing, eċċ.)
- Għarfien ta' l-evalwazzjoni tar-riskju u ta' implimentazzjonijiet prattiċi

Kompetenzi addizzjonali

- Rieda li taħdem 24x7 jew meta tiġi msejjaħ (skond il-mudell tas-servizz)
- Distanza massima ta' l-ivvjaġġar (f'każ ta' disponibilità ta' emerġenza fl-uffiċċju; ħin massimu ta' l-ivvjaġġar)
- Livell ta' edukazzjoni
- Esperjenza ta' xogħol fil-qasam tas-sigurtà ta' l-IT

CSIRT fittizju (pass 4)

Definizzjoni tal-Pjan tan-Negozju

Il-mudell finanzjarju

Minħabba l-fatt li l-kumpanija għandha e-kummerċ 24x7 kif ukoll dipartiment ta' l-IT 24x7, ġie deċiż li jkun ipprovdut servizz sħiħ waqt il-ħinijiet tax-xogħol u servizz *on call* għal wara l-ħinijiet tax-xogħol. Is-servizzi għall-kostitwenza se jkunu pprovduti bla ħlas, iżda l-possibilità li jingħataw servizzi lil klijenti esterni se tiġi evalwata matul il-fażi pilota u ta' l-evalwazzjoni.

Il-mudell tad-dħul

Matul il-fażi tal-bidu u l-fażi pilota l-CSIRT se jkun iffinanzjat permezz tal-kumpanija li tospitah. Matul il-fażi pilota u ta' l-evalwazzjoni se jiġi diskuss finanzjament addizzjonali, fosthom il-possibilità li jinbiegħu servizzi lil klijenti esterni.

Il-mudell organizzattiv
L-organizzazzjoni ospitanti hija kumpanija żgħira, għalhekk intgħażel il-mudell inkorporat. Waqt il-ħinijiet tax-xogħol, staff ta' tliet persuni ser jipprovdi s-servizzi bażiċi (għoti ta' pariri dwar is-sigurtà u immaniġġar/koordinament ta' l-inċidenti).

Id-dipartiment ta' l-IT tal-kumpanija diġà jħaddem persuni b'ħiliet adegwati. Sar ftehim ma' dak id-dipartiment sabiex il-CSIRT il-ġdid ikun jista' jitlob appoġġ fuq bażi ad-hoc meta jkun meħtieġ. Tista' tintuża wkoll it-tieni linja tat-teknixins *on call* tagħhom.
Se jkun hemm tim CSIRT bażiku b'erba' membri full-time u ħames membri addizzjonali tat-tim CSIRT. Wieħed minnhom se jkun disponibbli wkoll fuq xift li jdur.

Il-persunal
Il-mexxej tal-CSIRT għandu sfond fis-sigurtà u appoġġ ta' l-ewwel u t-tieni livell u għamel xogħol fil-qasam ta' l-immaniġġar ta' kriżi tar-reżistenza. It-tliet membri l-oħra tat-tim huma speċjalisti tas-sigurtà. Min-naħa tagħhom, il-membri tat-tim *part-time* tal-CSIRT mid-dipartiment ta' l-IT huma speċjalisti ta' l-infrastruttura tal-kumpanija.

L-użu u t-tagħmir ta' l-uffiċċju

It-tagħmir u l-użu ta' l-ispazju ta' l-uffiċċju u s-sigurtà fiżika huma suġġetti wiesgħa ħafna, u għalhekk ma tistax tingħata deskrizzjoni eżawrjenti f'dan id-dokument. Dan il-kapitlu huwa maħsub biex jagħti ħarsa ġenerali qasira ta' dan is-suġġett.

Aktar informazzjoni dwar is-sigurtà fiżika tista' tinstab fuq:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

"Tisħiħ tal-bini"
Peress li l-CSIRTs ġeneralment jimmaniġġaw informazzjoni sensittiva ħafna, hija prassi tajba li tħalli t-tim jieħu kontroll tas-sigurtà fiżika ta' l-uffiċċju. Dan se jiddependi ħafna fuq il-faċilitajiet u l-infrastruttura eżistenti u l-politika eżistenti dwar is-sigurtà ta' l-informazzjoni tal-kumpanija ospitanti.

Il-gvernijiet, per eżempju, jaħdmu bi skemi ta' klassifikazzjoni u huma stretti ħafna dwar kif tiġi mmaniġġata informazzjoni kunfidenzjali. Iċċekkja mal-kumpanija jew ma' l-istituzzjoni tiegħek dwar regoli u politiki lokali.

Ġeneralment CSIRT ġdid irid jiddependi fuq il-kooperazzjoni ta' l-organizzazzjoni li jkun fiha biex jitgħallem dwar ir-regoli u l-politiki lokali u kwistjonijiet oħra legali.

Deskrizzjoni komprensiva tat-tagħmir u l-miżuri tas-sigurtà kollha li se jkunu meħtieġa hija barra mill-iskop ta' dan id-dokument. Madankollu hawn taħt għandek issib lista qasira tal-faċilitajiet bażiċi għall-CSIRT tiegħek;

Regoli ġenerali għall-bini
- Uża kontrolli ta' l-aċċess
- Agħmel l-uffiċċju tal-CSIRT, talanqas, aċċessibbli biss għall-persunal tal-CSIRT.
- Issorvelja l-uffiċċji u d-daħliet b'kameras.
- Arkivja l-informazzjoni kunfidenzjali f'lokers jew f'sejf.
- Uża sistemi ta' l-IT siguri.

Regoli ġenerali għat-tagħmir ta' l-IT
- Uża tagħmir li l-persunal jista' jappoġġja
- Saħħaħ is-sistemi kollha
- Sewwi u aġġorna s-sistemi tiegħek kollha qabel ma tqabbadhom ma' l-internet
- Uża softwer tas-sigurtà (Firewalls, softwer kontra l-virusijiet, softwer kontra spyware, eċċ)

Żamma tal-kanali ta' komunikazzjoni
- Websajt Pubblika
- Żona riservata għall-membri fuq il-Websajt
- Formoli-web biex jiġu rrappurtati inċidenti
- Email (PGP / GPG / S/MIME support)
- Softwer għal-lista ta' l-impustar
- Ikollok numru tat-telefon iddedikat disponibbli għall-kostitwenza:
    - Telefon
    - Faks
    - SMS

Sistema(i) ta' intraċċar tar-rekords
- Database ta' kuntatti bid-dettalji tal-membri tat-tim, timijiet oħra, eċċ.
- Għodod CRM
- Sistema ta' biljett għall-immaniġġar ta' l-inċidenti

Uża l-'istil korporattiv' mill-bidu għal
- Preżentazzjoni standard għall-emails u l-bullettin tal-pariri
- Ittri 'konvenzjonali' fuq karta
- Ir-rapport ta' kull xahar jew annwali
- Il-formola għar-rappurtar ta' l-inċidenti

Kwistjonijiet oħra
- Ipprevedi komunikazzjoni barra l-faxxa f'każ ta' attakki
- Ipprevedi eċċessi fuq il-konnettività ta' l-internet

Għal aktar informazzjoni dwar għodod speċifiċi tal-CSIRT ara kapitlu *8.5 Għodod disponibbli għal CSIRT.*

Żvilupp ta' politika dwar is-sigurtà ta' l-informazzjoni

Jiddependi fuq it-tip ta' CSIRT, inti jkollok politika dwar is-sigurtà ta' l-informazzjoni adattata skond il-ħtiġijiet tiegħek. Minbarra li tiddeskrivi l-istat mixtieq tal-proċessi u l-proċeduri operattivi u amministrattivi, politika bħal din trid tkun konformi mal-leġislazzjoni u l-istandards, b'mod partikolari fir-rigward tar-responsabbiltà tal-CSIRT. Il-CSIRT normalment huwa marbut b'liġijiet u regolamenti nazzjonali, li ħafna drabi huma implimentati fil-kuntest ta' leġislazzjoni Ewropea (ġeneralment Direttivi) u ftehimiet internazzjonali oħra. L-istandards mhux bilfors jorbtu direttament, iżda jistgħu jiġu ordnati jew rakkomandati b'liġijiet u regolamenti.

Taħt hawn lista qasira ta' liġijiet u politiki possibbli:

Nazzjonali
- Diversi liġijiet dwar it-teknoloġija ta' l-informazzjoni, it-telekomunikazzjoni, il-medja
- Liġijiet dwar il-protezzjoni ta' l-informazzjoni u l-privatezza
- Liġijiet u regolamenti dwar iż-żamma ta' l-informazzjoni
- Leġislazzjoni dwar il-finanzi, il-kontabilità u l-ġestjoni korporattiva
- Kodiċijiet ta' mġiba għall-governanza korporattiva u l-governanza ta' l-IT

Ewropej
- Direttiva dwar il-firem elettroniċi (1999/93/KE)
- Direttivi dwar il-protezzjoni ta' l-informazzjoni (1995/46/KE) u l-privatezza f'komunikazzjonijiet elettroniċi (2002/58/KE)
- Direttivi dwar in-netwerks u servizzi ta' komunikazzjoni elettronika (2002/19/KE – 2002/22/KE)
- Direttivi dwar il-Liġi tal-Kumpaniji (eż. It-Tmien Direttiva dwar il-Liġi tal-Kumpaniji)

Internazzjonali
- Il-ftehim Basel II (speċjalment fir-rigward ta' l-immaniġġar ta' riskju operattiv)
- Il-Konvenzjoni tal-Kunsill ta' l-Ewropa dwar ir-Reati Ċibernetiċi
- Il-Konvenzjoni tal-Kunsill ta' l-Ewropa dwar id-Drittijiet tal-Bniedem (artikolu 8 dwar il-privatezza)
- Standards Internazzjonali tal-Kontabilità (IAS; sa ċertu punt huma jordnaw kontrolli ta' l-IT)

Standards
- L-Istandard Ingliż BS 7799 (Sigurtà ta' l-Informazzjoni)
- L-Istandards Internazzjonali ISO2700x (Sistemi għall-Immaniġġar tas-Sigurtà ta' l-Informazzjoni)
- L-IT-Grundschutzbuch Ġermaniż, L-EBIOS Franċiż u varjazzjonijiet nazzjonali oħra

Biex tistabbilixxi jekk il-CSIRT tiegħek hux qiegħed jaġixxi skond il-leġislazzjoni nazzjonali u internazzjonali, jekk jogħġbok ikkonsulta lill-konsulent legali tiegħek.

L-aktar mistoqsijiet bażiċi li jridu jiġu mwieġba fil-politiki dwar l-immaniġġar ta' l-informazzjoni tiegħek huma:

- L-informazzjoni li tidħol kif tiġi "mmarkata" jew "ikklassifikata"?
- Kif tiġi mmaniġġata l-informazzjoni, speċjalment fir-rigward ta' l-esklussività?
- X'kunsiderazzjonijiet huma adottati għall-iżvelar ta' informazzjoni, b'mod speċjali jekk tiġi mgħoddija informazzjoni relatata ma' inċident lil timijiet jew siti oħra?
- Hemm konsiderazzjonijiet legali li jridu jitqiesu fir-rigward ta' l-immaniġġar ta' l-informazzjoni?
- Għandek politika dwar l-użu ta' kriptografija biex tipproteġi l-esklussività u l-integrità fl-arkivji u/jew fil-komunikazzjoni ta' l-informazzjoni, speċjalment e-mail?
- Din il-politika tinkludi kundizzjonijiet possibbli ta' limitu legali bħall-kustodja tal-*keys* jew l-infurzar tad-dekodifikazzjoni f'każ ta' taħrikiet?

CSIRT fittizju (pass 5)

It-tagħmir ta' l-uffiċċju u l-post

Minħabba li l-kumpanija ospitanti diġà għandha sigurtà fiżika effiċjenti fis-seħħ, il-CSIRT il-ġdid huwa kopert sewwa f'dak ir-rigward. Hekk imsejħa "kamra tal-gwerra" hija pprovduta sabiex tippermetti koordinazzjoni f'każ ta' emerġenza. Inxtara sejf għall-materjal kodifikat u dokumenti sensittivi. Ġiet stabbilita linja tat-telefon separata li tinkludi swiċċbord biex jiffaċilita l-*hotline* waqt il-ħinijiet tax-xogħol u t-telefon mobbli "*on-call*" għall-ħin barra l-ħinijiet tax-xogħol bl-istess numru tat-telefon.

Jista' jintuża wkoll tagħmir eżistenti u l-websajt korporattiva biex tixxandar informazzjoni relatata mal-CSIRT. Hija installata u miżmuma lista ta' l-impustar, b'parti ristretta għall-komunikazzjoni bejn il-membri tat-tim u ma' timijiet oħra. Id-dettalji ta' kuntatt tal-membri tal-persunal huma maħżuna f'database, b'kopja stampata miżmuma fis-sejf.

Regolament

Minħabba l-fatt li l-CSIRT huwa inkorporat f'kumpanija li diġà għandha politiki dwar is-sigurtà ta' l-informazzjoni, il-politiki relattivi għall-CSIRT ġew stabbiliti bl-għajnuna tal-konsulent legali tal-kumpanija.

Tiftix għal kooperazzjoni bejn CSIRTs oħra u inizjattivi nazzjonali possibbli

L-eżistenza ta' inizjattivi ta' CSIRTs oħra u l-ħtieġa qawwija ta' kooperazzjoni bejniethom diġà ssemmiet diversi drabi f'dan id-dokument. Hija prattika tajba li tikkuntattja CSIRTs oħra kemm jista' jkun malajr biex tikseb il-kuntatt neċessarju mal-komunitajiet CSIRT. Ġeneralment CSIRTs oħra huma lesti ħafna li jgħinu timijiet ġodda li għadhom jiffurmaw sabiex jibdew.

L-*Inventarju ta' l-attivitajiet CERT fl-Ewropa*[14] ta' ENISA huwa punt ta' tluq tajjeb ħafna biex tfittex CSIRTs oħra fil-pajjiż jew attivitajiet ta' kooperazzjoni tal-CSIRT nazzjonali.

Biex tikseb għajnuna sabiex issib sors xieraq ta' informazzjoni dwar il-CSIRT, ikkuntattja lill-esperti dwar il-CSIRT ta' l-ENISA:

CERT-Relations@enisa.europa.eu

[14] Inventarju ta' l-ENISAs: http://www.enisa.europa.eu/cert_inventory/

Din li ġejja hija ħarsa ġenerali fil-qosor ta' l-attivitajiet tal-komunità CSIRT. Jekk jogħġbok irreferi għall-*Inventarju* għal deskrizzjoni aktar komprensiva u aktar tagħrif.

Inizjattiva ta' CSIRT Ewropew

TF-CSIRT[15]

It-Task Force TF-CSIRT jippromwovi l-kollaborazzjoni bejn it-Timijiet ta' Rispons għall-Inċidenti tal-Kompjuter (CSIRTs) fl-Ewropa. L-għanijiet prinċipali ta' din it-Task Force huma li tipprovdi forum għall-iskambju ta' esperjenzi u għarfien, li tistabbilixxi servizzi pilota għall-komunità Ewropea tal-CSIRTs u tassisti l-istabbiliment ta' CSIRTs ġodda.

L-għanijiet prinċipali tat-Task Force huma:

- Li tipprovdi forum sabiex jiġu skambjati esperjenzi u għarfien
- Li tistabbilixxi servizzi pilota għall-komunità tal-CSIRTs Ewropej
- Li tippromwovi standards u proċeduri komuni bi tweġiba għall-inċidenti ta' sigurtà
- Li tassisti fl-istabbiliment ta' CSIRTs ġodda u t-taħriġ tal-persunal tal-CSIRTs.
- L-attivitajiet tat-TF-CSIRT huma ffukati fuq l-Ewropa u l-pajjiżi ġirien, skond it-Termini ta' Referenza approvati mill-Kumitat Tekniku TERENA fil-15 ta' Settembru 2004.

Inizjattiva ta' CSIRT globali

FIRST[16]

FIRST hija l-organizzazzjoni primarja u l-gwida globali rikonoxxuta fir-rispons għall-inċidenti. Sħubija f'FIRST tippermetti lit-timijiet ta' rispons għall-inċidenti li jwieġbu b'mod effettiv għall-inċidenti ta' sigurtà – b'mod reattiv kif ukoll proattiv.

FIRST tlaqqa' flimkien varjetà ta' timijiet ta' rispons għall-inċidenti ta' sigurtà tal-kompjuter minn organizzazzjonijiet governattivi, kummerċjali, u edukattivi. FIRST timmira li tkabbar il-kooperazzjoni u l-koordinament fil-prevenzjoni ta' l-inċidenti, li tistimula reazzjoni rapida għall-inċidenti, u li tippromwovi l-qsim ta' informazzjoni bejn il-membri u l-komunità b'mod ġenerali.

Apparti min-netwerk ta' fiduċja li FIRST tifforma fil-komunità globali ta' rispons għall-inċidenti, FIRST tipprovdi wkoll servizzi ta' valur miżjud.

CSIRT fittizju (pass 6)
Tiftix għal kooperazzjoni Bl-użu ta' l-Inventarju ta' ENISA, xi CSIRTs fl-istess pajjiż malajr instabu u ġew ikkuntattjati. Ġiet irranġata żjara fuq il-post ma' wieħed minnhom għall-mexxej tat-tim li ġie mqabbad. Huwa tgħallem dwar l-attivitajiet tal-CSIRT nazzjonali u attenda laqgħa. Din il-laqgħa kienet aktar minn utli biex jiġbor eżempji ta' metodi ta' ħidma u jikseb appoġġ minn għadd ta' timijiet oħra.

[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 Promozzjoni tal-Pjan Korporattiv

Sa issa għamilna dawn il-passi:

1. Ftehim ta' x'inhu CSIRT u x'benefiċċji jista' jipprovdi.
2. Lil liema settur ser jipprovdi s-servizzi tiegħu t-tim il-ġdid?
3. X'tipi ta' servizzi jista' jipprovdi CSIRT lill-kostitwenza tiegħu.
4. Analiżi ta' l-ambjent u l-kostitwenti.
5. Definizzjoni tad-dikjarazzjoni tal-missjoni
6. Żvilupp tal-Pjan Korporattiv
    a. Definizzjoni tal-mudell finanzjarju
    b. Definizzjoni ta' l-istruttura organizzattiva
    ċ. Bidu ta' tħaddim tal-persunal
    d. Użu u tagħmir ta' l-uffiċċju
    e. Żvilupp ta' politika dwar is-sigurtà ta' l-informazzjoni
    f. Tfittxija għal sħab ta' kooperazzjoni

>> Il-pass li jmiss huwa li dan ta' hawn fuq jitpoġġa fi pjan tal-proġett u nibdew!

Bidu tajjeb biex tiddefinixxi l-proġett tiegħek huwa li tipproduċi pjan korporattiv. Dan il-pjan korporattiv jintuża bħala bażi għall-pjan tal-proġett u jintuża wkoll biex tapplika għal appoġġ tat-tmexxija u tikseb baġit jew riżorsi oħra.

Instab utli biex wieħed jirrapporta kontinwament lit-tmexxija bil-għan li jinżamm għarfien għoli dwar il-problemi tas-sigurtà fl-IT u permezz ta' dan għal appoġġ kontinwu għall-CSIRT tiegħu.

Il-bidu ta' pjan korporattiv jibda bl-analiżi tal-problemi u l-opportunitajiet bl-użu ta' mudell ta' analiżi, deskritt f'kapitlu *5.3 Analiżi tal-kostitwenza*, u tfittxija ta' kuntatt mill-qrib mal-kostitwenza.

Kif deskritt aktar qabel, hemm ħafna dwar xiex wieħed jaħseb meta jinbeda CSIRT. L-aħjar li jsir aġġustament tal-materjal hawn fuq imsemmi skond il-ħtiġijiet tal-CSIRTs hekk kif jiżviluppaw.

Hija prattika tajba, meta wieħed jirrapporta lit-tmexxija, li jagħmel il-każ proprju aġġornat kemm jista' jkun billi jintużaw artikli mill-gazzetti jew l-internet u jiġi spjegat għaliex is-servizz ta' CSIRT u l-koordinament intern ta' l-inċidenti huma kruċjali għal assi tan-negozju siguri. Huwa neċessarju wkoll li wieħed jagħmilha ċara li appoġġ kontinwu biss fi kwistjonijiet ta' sigurtà ta' l-IT iwassal għal negozju stabbli, speċjalment għal kumpanija jew istituzzjoni li hija dipendenti fuq l-IT.

(Fażi prominenti minn Bruce Schneier tispjega sewwa dan il-punt: "Is-sigurtà mhijiex prodott iżda proċess[17]*!*")

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

Għodda famuża biex tillustra l-problemi tas-sigurtà hija t-tabella segwenti pprovduti mill-CERT/CC:

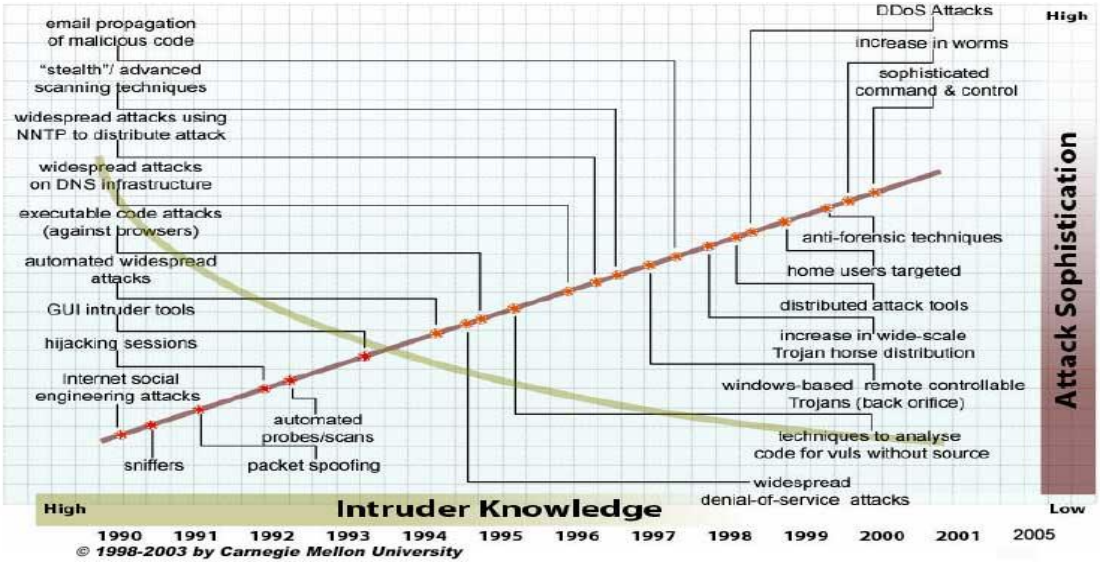


Fig. 8 Għarfien ta' l-intruż kontra s-sofistikazzjoni ta' l-attakki (sors CERT-CC[18])

Hija turi x-xejriet fis-sigurtà ta' l-IT, speċjalment it-tnaqqis fil-ħiliet neċessarji biex jitwettqu attakki dejjem aktar sofistikati. It

Punt ieħor li għandu jissemma huwa ż-żmien dejjem anqas bejn id-disponibilità ta' l-aġġornamenti tas-softwer kontra l-vulnerabilitajiet u l-bidu ta' l-attakki kontriehom:

Patch -> Exploit		**Rata ta' tixrid**	
Nimda:	11-il xahar	Code red:	Ġranet
Slammer:	6 xhur	Nimda:	Sigħat
Nachi:	5 xhur	Slammer:	Minuti
Blaster:	3 ġimgħat		
Witty:	ġurnata (!)		

L-informazzjoni miġbura dwar l-inċidenti, it-titjib li jista' jseħħ u l-lezzjonijiet meħuda wkoll jagħmlu preżentazzjoni tajba.

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

Deskrizzjoni tal-pjanijiet korporattivi u stimoli amministrattivi

Preżentazzjoni għat-tmexxija li tinkludi l-promozzjoni tal-CSIRT waħedha ma tagħmilx każ korporattiv, iżda jekk issir b'mod xieraq hija twassal għal appoġġ mit-tmexxija għall-CSIRT fil-biċċa l-kbira tal-każijiet. Mill-banda l-oħra, il-każ korporattiv m'għandux jitqies sempliċement bħala eżerċizzju ta' amministrazzjoni iżda għandu jintuża wkoll għall-komunikazzjoni mat-tim u l-kostitwenza. It-terminu każ korporattiv jista' jinstema' kummerċjali ħafna u 'l bogħod ferm mill-prattika ta' kuljum ta' CSIRT, iżda jipprovdi konċentrazzjoni u direzzjoni tajba meta jitwaqqaf CSIRT.

It-tweġibiet għall-mistoqsijiet li ġejjin jistgħu jintużaw biex jitfassal pjan korporattiv tajjeb (l-eżempji mogħtija huma ipotetiċi u użati sempliċement għal illustrazzjoni. It-tweġibiet "reali" huma dipendenti ħafna fuq iċ-ċirkustanzi "reali").

- X'inhi l-problema?
- X'tixtieq tikseb mal-kostitwenti tiegħek?
- X'jiġri jekk ma tagħmel xejn?
- X'jiġri jekk tieħu azzjoni?
- X'se jkun il-prezz?
- X'se jkun il-gwadann?
- Meta se tibda u meta tispiċċa?

X'inhi l-problema?
F'ħafna każijiet l-idea li jitwaqqaf CSIRT tqum meta s-sigurtà ta' l-IT tkun saret parti vitali tan-negozju prinċipali ta' kumpanija jew istituzzjoni u meta l-inċidenti ta' sigurtà fl-IT isiru riskju tan-negozju, li jagħmel it-titjib tas-sigurtà operazzjoni normali tan-negozju.

Il-maġġoranza tal-kumpaniji jew istituzzjonijiet għandhom dipartiment regolari ta' appoġġ jew *helpdesk* iżda fil-biċċa l-kbira tal-każijiet l-inċidenti tas-sigurtà jiġu mmaniġġati b'mod insuffiċjenti u mhux strutturati daqs kemm għandu jkun. Fil-maġġoranza tal-każijiet, il-qasam tax-xogħol ta' l-inċidenti tas-sigurtà jeħtieġ ħiliet u attenzjoni speċjali. Li jkollok approċċ aktar strutturat huwa wkoll ta' benefiċċju u jnaqqas ir-riskji kummerjċali u korporattivi u l-ħsara lill-kumpanija.

Il-problema fil-maġġoranza tal-każijiet hija li hemm nuqqas ta' koordinazzjoni u li għerf eżistenti ma jintużax biex jiġu mmaniġġati l-inċidenti, li jista' jimpedihom milli jseħħu fil-ġejjieni u jiġu evitati telf finanzjarju possibbli u / jew ħsara lir-reputazzjoni ta' istituzzjoni.

X'inhuma l-miri li jridu jinkisbu mal-kostitwenza?
Kif spjegat aktar qabel, il-CSIRT tiegħek se jservi lill-kostitwenti tiegħu u jassistihom biex isolvu problemi u inċidenti ta' sigurtà fl-IT. It-tkabbir tal-livell ta' l-għarfien dwar is-sigurtà ta' l-IT u l-ksib ta' kultura ta' għarfien dwar is-sigurtà huma miri addizzjonali.

Din il-kultura tipprova miżuri proattivi u preventivi meħuda mill-bidu u għalhekk tnaqqas l-ispejjeż operattivi.

L-introduzzjoni ta' din il-kultura ta' kooperazzjoni u assistenza lil kumpanija jew istituzzjoni tista' f'ħafna każijiet tistimula l-effiċjenza b'mod ġenerali.

X'jiġri jekk ma jsir xejn?
Mod mhux strutturat ta' ġestjoni tas-sigurtà ta' l-IT jista' jwassal għal aktar ħsara, mhux l-anqas lir-reputazzjoni tal-kumpanija. It-telf finanzjarju u l-implikazzjonijiet legali jistgħu jkunu riżultati oħra.

X'jiġri jekk tittieħed azzjoni?
L-għarfien dwar is-seħħ ta' problemi tas-sigurtà jikber. Dan jgħin biex jiġu solvuti b'mod aktar effiċjenti u jiġi evitat telf futur.

X'se jkun il-prezz?
Jiddependi fuq il-mudell organizzattiv, l-ispejjeż involuti se jkunu s-salarji tal-membri u l-organizzazzjoni tat-tim CSIRT, it-tagħmir, l-għodod u l-liċenzji tas-softwer.

X'se jkun il-gwadann?
Jiddependi fuq in-negozju u t-telf fil-passat, se tikseb aktar trasparenza fil-proċeduri u l-prattiċi tas-sigurtà, u b'hekk tipproteġi assi tan-negozju essenzjali.

X'inhi l-kronoloġija?
Ara kapitlu *12. Deskrizzjoni tal-Pjan tal-proġett* għad-deskrizzjoni ta' kampjun ta' pjan ta' proġett.

Eżempji ta' każijiet tan-negozju u approċċi eżistenti
Hawnhekk hawn xi eżempji għal każijiet tan-negozju CSIRT li ta' min jistudjahom:

- http://www.cert.org/csirts/AFI_case-study.html
  Ħolqien ta' CSIRT ta' Istituzzjoni Finanzjarja: Studju tal-Każ

L-għan ta' dan id-dokument huwa li jiġu maqsuma l-lezzjonijiet meħuda minn istituzzjoni finanzjarja (imsemmija f'dan id-dokument bħala AFI) hekk kif żviluppaw u implimentaw kemm pjan biex jiġi indirizzat tħassib tas-sigurtà kif ukoll Tim ta' Rispons għall-Inċidenti ta' Sigurtà tal-Kompjuter (CSIRT).

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Sommarju tal-każ korporattiv ta' CERT POLSKA (wirja ta' slajds f'format PDF).

- http://www.auscert.org.au/render.html?it=2252
  Li tifforma Tim ta' Rispons għall-Inċidenti (IRT) fl-1990s tista' tkun biċċa xogħol li taqta' qalb dak li jkun. Ħafna nies li jiffurmaw IRT m'għandhomx esperjenza f'li jagħmlu dan. Dan id-dokument jeżamina r-rwol li IRT jista' jilgħab fil-komunità, u l-kwistjonijiet li għandhom jiġu indirizzati kemm waqt il-ħolqien u wara l-bidu ta' l-operazzjonijiet. Jista' jkun utli għal IRTs eżistenti billi jista' jkabbar l-għarfien dwar kwistjonijiet li ma ġewx indirizzati qabel.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Studju tal-Każ dwar is-Sigurtà ta' l-Informazzjoni, Kif tagħmel l-intrapriża sigura, Minn: Roger Benton

  Dan il-prattiku huwa studju tal-każ tal-migrazzjoni ta' Kumpanija ta' l-Assigurazzjoni għal sistema ta' sigurtà għall-intrapriża kollha. Huwa l-ħsieb ta' dan il-prattiku li jipprovdi linja li għandha tiġi segwita meta tinħoloq jew issir migrazzjoni għal sistema ta' sigurtà. Fil-bidu, sistema ta' sigurtà primittiva onlajn kienet l-uniku mekkaniżmu biex tikkontrolla l-aċċess għall-informazzjoni korporattiva. L-esponimenti kienu serji – ma kien hemm ebda kontrolli ta' l-integrità barra mill-ambjent onlajn. Kwalunkwe persuna b'ħiliet bażiċi fl-ipprogrammar seta' jżid, jibdel u/jew iħassar informazzjoni tal-produzzjoni.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Strateġija dwar l-e-sigurtà ta' Marriott: kollaborazzjoni bejn in-negozju u l-IT

  L-esperjenza ta' Chris Zoladz ta' Marriott International Inc., is-sigurtà ta' l-e-negozju hija proċess, mhux proġett. Dan kien il-messaġġ li wassal Zoladz fil-Konferenza u Expo riċenti dwar l-E-Sigurtà ġewwa Boston, sponsorjata mill-Intermedia Group. Bħala viċi-president tal-protezzjoni ta' l-informazzjoni għal Marriott, Zoladz jirrapporta permezz tad-dipartiment legali, għalkemm mhuwiex avukat. Il-funzjoni tiegħu hija li jidentifika fejn hija maħżuna l-aktar informazzjoni kummerċjali prezzjuża ta' Marriott u kif din timxi ġewwa u barra l-kumpanija. Marriott għandha responsabbiltà separata definita għall-infrastruttura teknika li tappoġġja s-sigurtà, li hija mogħtija lill-arkitett tas-sigurtà ta' l-IT.

CSIRT fittizju (pass 7)

Promozzjoni tal-Pjan Korporattiv

Ġie deċiż li jinġabru fatti u figuri mill-istorja tal-kumpanija. Dan huwa aktar minn utli għal ħarsa ġenerali statistika tas-sitwazzjoni tas-sigurtà ta' l-IT. Dan il-ġbir għandu jissokta meta l-CSIRT ikun beda jiffunzjona, sabiex l-istatistika tinżamm aġġornata.

Ġew ikkuntattjati u intervistati CSIRTs nazzjonali oħra dwar il-każijiet tan-negozju tagħhom. Huma pprovdew appoġġ billi kkompilaw xi slajds b'informazzjoni dwar żviluppi riċenti fl-inċidenti tas-sigurtà ta' l-IT u dwar l-ispejjeż ta' l-inċidenti.

F'dan il-każ ta' eżempju ta' CSIRT fittizju ma kienx hemm ħtieġa kbira li t-tmexxija tiġi konvinta dwar l-importanza tan-negozju ta' l-IT, u għalhekk ma kienx diffiċli sabiex tinkiseb l-awtorizzazzjoni għall-ewwel pass. Ġew imħejjija każ tan-negozju u pjan tal-proġett, fosthom stima ta' l-ispejjeż tat-twaqqif u l-prezz ta' l-operazzjoni.

8 Eżempji ta' proċeduri operattivi u tekniċi (flussi tax-xogħol)

Sa issa għamilna l-passi li ġejjin:

1. Ftehim ta' x'inhu CSIRT u x'benefiċċji jista' jipprovdi.
2. Lil liema settur ser jipprovdi s-servizzi tiegħu t-tim il-ġdid?
3. X'tipi ta' servizzi jista' jipprovdi CSIRT lill-kostitwenza tiegħu.
4. Analiżi ta' l-ambjent u l-kostitwenti.
5. Definizzjoni tad-dikjarazzjoni tal-missjoni.
6. Żvilupp tal-Pjan tan-Negozju.
   a. Definizzjoni tal-mudell finanzjarju.
   b. Definizzjoni ta' l-istruttura organizzattiva.
   ċ. Bidu ta' tħaddim tal-persunal.
   d. Użu u tagħmir ta' l-uffiċċju.
   e. Żvilupp ta' politika dwar is-sigurtà ta' l-informazzjoni.
   f. Tfittxija għal sħab ta' kooperazzjoni.
7. Promozzjoni tal-Pjan tan-Negozju.
   a. Approvazzjoni tal-każ tan-negozju.
   b. Daħħal kollox fi pjan tal-proġett.

>> Il-pass li jmiss: li tagħmel il-CSIRT jiffunzjona

Li jkollok flussi tax-xogħol definiti sewwa fis-seħħ itejjeb il-kwalità u l-ħin meħtieġ għal kull inċident jew każ ta' vulnerabilità.

Kif deskritt fil-kaxxi ta' l-eżempju, CSIRT Fittizju se joffri s-servizzi prinċipali bażiċi ta' CSIRT:

- Allarmi u Twissijiet
- Immaniġġar ta' l-Inċidenti
- Dikjarazzjonijiet

Dan il-kapitlu jipprovdi eżempji ta' flussi tax-xogħol li jiddeskrivu s-servizzi prinċipali ta' CSIRT. Dan il-kapitlu fih ukoll tagħrif dwar il-ġbir ta' informazzjoni minn sorsi differenti, l-iċċekkjar tagħha għar-rilevanza u l-awtentiċità u t-tqassim mill-ġdid tagħha lill-kostitwenza. U fl-aħħarnett dan il-kapitlu fih eżempji ta' l-aktar proċeduri bażiċi u għodod speċifiċi ta' CSIRT.

Evalwa l-bażi ta' l-installazzjoni tal-kostitwenza tiegħek

L-ewwel pass huwa li tiġbor deskrizzjoni ġenerali tas-sistemi ta' l-IT installati fil-kostitwenza tiegħek. Permezz ta' dan il-CSIRT jista' jevalwa r-rilevanza ta' l-informazzjoni li tidħol u jiffiltraha qabel ma terġa' titqassam, għalhekk il-kostitwenti ma jiġux mgħarrqa b'informazzjoni li prattikament tkun bla użu għalihom.

Hija prattika tajba li tibda sempliċi, per eżempju billi tuża folja ta' l-excel bħal din:

Kategorija	Applikazzjoni	Prodott tas-softwer	Verżjoni	OS	Verżjoni ta' l-OS	Kostitwent
Desktop	Office	Excel	x-x-x	Microsoft	XP-prof	A
Desktop	Browser	IE	x-x-	Microsoft	XP-prof	A
Network	Router	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Servizzi	Server tal-Web	Apache		Unix	x-x-x	B

Bil-funzjoni tal-filter fl-excel huwa faċli ħafna biex tagħżel is-softwer adatt u tara liema kostitwent qed juża liema tip ta' softwer.

Produzzjoni ta' Allarmi, Twissijiet u Dikjarazzjonijiet

Il-produzzjoni ta' l-allarmi, twissijiet u dikjarazzjonijiet kollha jsegwu l-istess flussi tax-xogħol:

- Il-ġbir ta' l-informazzjoni
- Evalwazzjoni ta' l-informazzjoni għar-rilevanza u s-sors
- Stima tar-riskju bbażata fuq l-informazzjoni miġbura
- Tqassim ta' l-informazzjoni

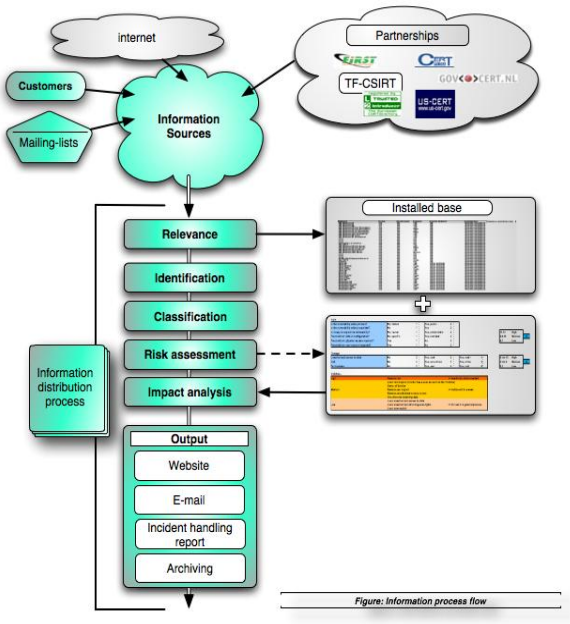


Fig. 9 : Fluss tal-proċess ta' l-informazzjoni

Fil-paragrafi li ġejjin dan il-fluss tax-xogħol se jiġi deskritt f'aktar dettall.

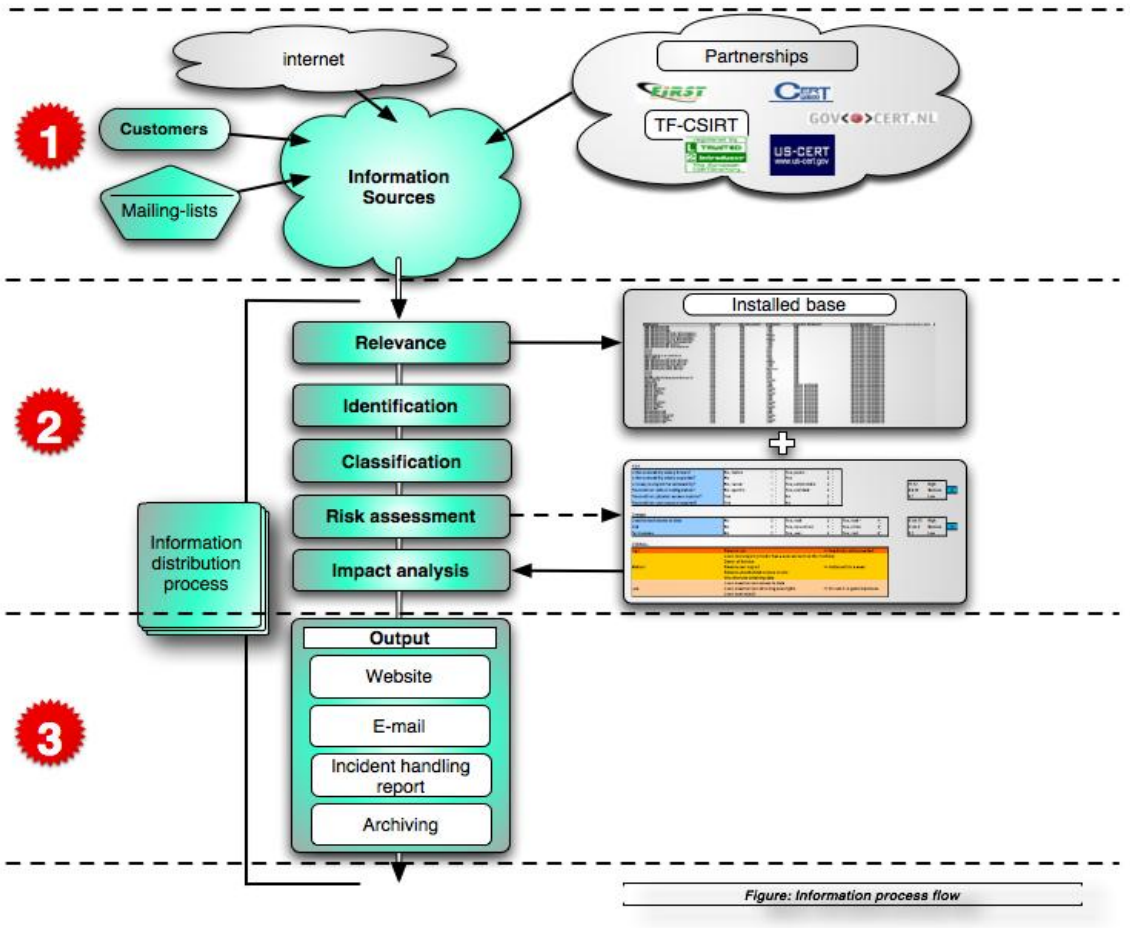


Figure: Information process flow

1 Pass 1: Ġbir ta' informazzjoni dwar il-vulnerabilità.

Normalment jeżistu żewġ tipi ewlenin ta' sorsi ta' informazzjoni li jikkontribwixxu tagħrif bħala input għas-servizzi:

- L-informazzjoni tal-vulnerabilità dwar is-sistemi ta' l-IT (tiegħek)
- Ir-rapporti ta' l-inċidenti

Jiddependi fuq it-tip ta' negozju u infrastruttura ta' l-IT, jista' jkun hemm bosta sorsi pubbliċi u magħluqa għal informazzjoni dwar il-vulnerabilità:

- Listi ta' l-impustar pubbliċi u magħluqa
- Informazzjoni dwar il-vulnerabilità tal-prodott mill-bejjiegħ
- Websajts
- Informazzjoni fuq l-internet (Google, eċċ…)
- Sħubijiet pubbliċi u privati li jipprovdu informazzjoni dwar il-vulnerabilità (FIRST, TF-CSIRT, CERT-CC, US-CERT….)

Din l-informazzjoni kollha tikkontribwixxi għal-livell ta' għarfien dwar vulnerabilitajiet speċifiċi fis-sistemi ta' l-IT.

Kif intqal qabel, hemm ħafna sorsi ta' informazzjoni tajbin u faċilment aċċessibbli dwar is-sigurtà disponibbli fuq l-internet. Il-grupp ta' ħidma ad-hoc ta' ENISA "Servizzi CERT" għall-2006 qiegħed jipproduċi f'dan il-waqt lista aktar komprensiva li suppost tkun lesta fit-tmiem ta' l-2006[19].

Pass 2: Evalwazzjoni ta' l-informazzjoni u stima tar-riskju

Dan il-pass jirriżulta f'analiżi ta' l-impatt ta' vulnerabilità speċifika għall-infrastruttura ta' l-IT tal-kostitwenza.

Identifikazzjoni
L-informazzjoni li tidħol dwar il-vulnerabilità dejjem trid tiġi identifikata bis-sors tagħha u jrid jiġi stabbilit jekk is-sors huwiex affidabbli qabel ma tingħata xi informazzjoni lill-kostitwenza. Inkella n-nies jistgħu jiġu allarmati bi żball, li jista' jwassal għal disturbi bla bżonn fil-proċessi tan-negozju u finalment għal dannu fir-reputazzjoni tal-CSIRT.

[19] Grupp ta' Ħidma Ad-hoc Servizzi CERT:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Il-proċedura li ġejja turi eżempju ta' kif tiġi identifikata l-awtenticità ta' messaġġ:

Proċedura biex tidentifika l-awtenticità ta' messaġġ u s-sors tiegħu

Lista ta' Kontroll (Checklist) Ġenerali
1. Is-sors huwa magħruf u rreġistrat bħala tali?
2. L-informazzjoni ġejja minn kanal regolari?
3. Hemm informazzjoni "stramba" kontenuta li tinħass "mhix sewwa"?
4. Segwi l-istint tiegħek, jekk hemm dubju dwar informazzjoni, taġixxix, iżda erġa' ivverifika!

Sorsi ta' l-Emails
1. L-indirizz tas-sors huwa magħruf għall-organizzazzjoni u magħruf għal-lista tas-sorsi?
2. Il-firma PGP hija korretta?
3. Meta jkollok dubju, iċċekkja t-titolu kollha ta' messaġġ.
4. Meta jkollok dubju, uża "nslookup" jew "dig" biex tivverifika d-*domain* ta' min ikun bagħat[20].

Sorsi tal-WWW
1. Iċċekkja ċ-ċertifikati tal-brawżer meta taqbad ma' websajt *secured* (https ://).
2. Iċċekkja s-sors għall-kontenut u l-validità (teknika).
3. Meta jkollok dubju, tikklikkja fuq ebda *link* jew tniżżel xi softwer.
4. Meta jkollok dubju, agħmel "lookup" u "dig" fuq id-*domain* u agħmel "traceroute".

Telefon
1. Isma' l-isem sewwa.
2. Għaraftha l-vuċi?
3. Meta jkollok dubju, staqsi għal numru tat-telefon u itlob biex terġa' ċċempel lil min ikun qiegħed fuq il-linja.

Fig. 10 Eżempju ta' proċedura għall-identifikazzjoni ta' l-informazzjoni

Rilevanza
Il-ħarsa ġenerali prodotta qabel tal-ħardwer u tas-softwer installat tista' tintuża biex tiġi ffiltrata l-informazzjoni li tkun dieħla tal-vulnerabilità għar-rilevanza, bil-għan li tinstab tweġiba għall-mistoqsijiet: "Il-kostitwenza tuża din il-biċċa softwer?"; "L-informazzjoni hija rilevanti għalihom?"

Klassifikazzjoni
Xi informazzjoni riċevuta tista' tiġi kklassifikata jew immarkata bħala ristretta (per eżempju rapporti ta' inċidenti li jidħlu minn timijiet oħra). L-informazzjoni kollha trid tiġi mmaniġġjata skond id-domanda ta' min jibgħatha u skond il-politika dwar is-sigurtà ta' l-informazzjoni tiegħu stess. Regola bażika tajba hija "Tqassamx informazzjoni jekk ma jkunx ċar li hija intenzjonata biex titqassam; f'każ ta' dubju staqsi lil min ikun bagħat l-informazzjoni għall-permess biex tagħmel dan."

[20] Għodod biex jiġu ċċekkjati l-identitajiet fil-CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Stima tar-riskju u analiżi ta' l-impatt
Hemm diversi metodi biex tistabbilixxi r-riskju u l-impatt ta' vulnerabilità (potenzjali).

Riskju huwa definit bħala ċ-ċans potenzjali li l-vulnerabilità tista' tiġi sfruttata. Hemm diversi fatturi importanti (fost l-oħrajn):

- Il-vulnerabilità hija magħrufa sewwa?
- Il-vulnerabilità mifruxa ħafna?
- Faċli tisfrutta l-vulnerabilità?
- Din hija tip ta' vulnerabilità li bil-mod biex tiġi sfruttata?

Dawn il-mistoqsijiet kollha jagħtu idea tajba tas-serjetà tal-vulnerabilità.
Approċċ sempliċi ħafna biex tikkalkula r-riskju hija l-formula li ġejja:

Impatt = Ħsara potenzjali minn Riskju X

Ħsara potenzjali tista' tkun

- Aċċess mhux awtorizzat għall-informazzjoni
- Ċaħda tas-Servizz (DOS)
- Ksib jew estensjoni tal-permessi

(Għal skemi ta' klassifikazzjoni aktar elaborati jekk jogħġbok ara t-tmiem ta' dan il-kapitlu).

B'dawn il-mistoqsijiet imwieġba tista' tiżdied valutazzjoni globali mal-konsulenza, li tinforma dwar ir-riskju u d-dannu potenzjali. Ħafna drabi jintużaw termini sempliċi bħal BAXX, MEDJU u GĦOLI.

Skemi oħra, aktar komprensivi ta' evalwazzjoni tar-riskju huma:

L-iskema ta' valutazzjoni ta' GOVCERT.NL[21]
Il-CSIRT governattiv Olandiż GOVCERT.NL żviluppa matriċi għall-evalwazzjoni tar-riskju li ġiet żviluppata fil-faża tal-bidu ta' Govcert.nl u għadha tiġi aġġornata għall-aħħar xejriet.

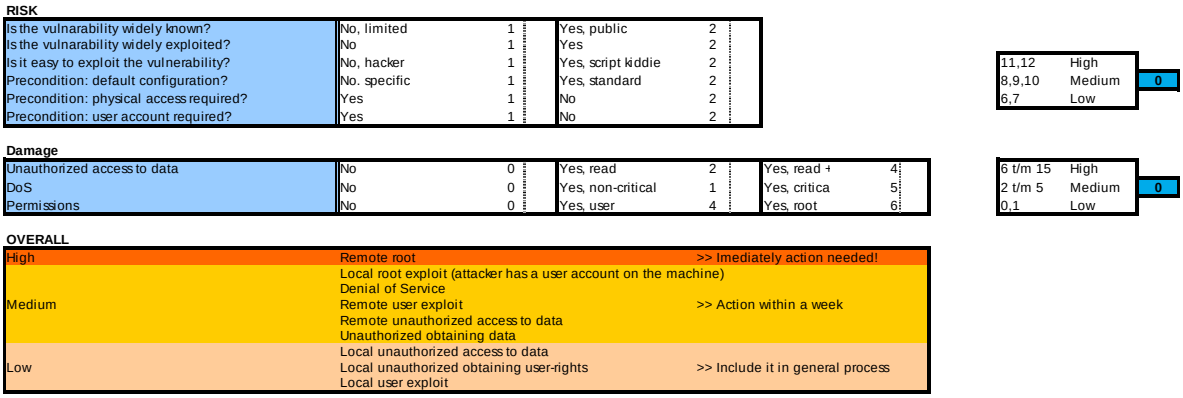


Fig. 11 L-iskema ta' valutazzjoni ta' GOVCERT.NL

Deskrizzjoni tal-Format ta' Konsulenza Komuni ta' l-EISPP[22]
Il-Programm Ewropew ta' Informazzjoni dwar is-Sigurtà ta' l-Informazzjoni (EISPP) huwa proġett ko-finanzjat mill-Komunità Ewropea taħt il-Ħames Programm ta' Qafas. Il-proġett ta' l-EISPP jimmira li jiżviluppa qafas Ewropew, mhux biss biex jiġi maqsum għarfien dwar is-sigurtà iżda wkoll biex jiġu definiti l-kontenut u modi kif titwassal l-informazzjoni dwar is-sigurtà lill-SMEs. Bil-provvediment tas-servizzi ta' sigurtà neċessarji ta' l-IT lill-SMEs Ewropej, dawn jiġu inkoraġġiti sabiex jiżviluppaw il-fiduċja u l-użu tagħhom ta' l-e-kummerċ li jwassal għal opportunitajiet akbar u aħjar għal negozju ġdid. L-EISPP huwa pijunier fil-viżjoni tal-Kummissjoni Ewropea ta' ħolqien ta' netwerk Ewropew ta' kompetenza fi ħdan l-Unjoni Ewropea.

Il-Format tal-Konsulenza tad-DAF Deutsches[23]
DAF hija inizjattiva tal-CERT-Verbund Ġermaniż u hija parti prinċipali ta' infrastruttura għall-ħolqien u skambju ta' konsulenzi dwar is-sigurtà minn timijiet differenti. DAF hija magħmula b'mod speċjali għall-ħtiġijiet tal-CERTs Ġermaniżi; l-istandard huwa żviluppat u miżmum minn CERT-Bund, DFN-CERT, PRESECURE u Siemens-CERT.

[21] Matriċi tal-vulnerabilità: 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

Pass 3: Tqassim ta' l-informazzjoni

CSIRT jista' jagħżel minn diversi metodi ta' distribuzzjoni skond ix-xewqat tal-kostitwenti u l-istrateġija tiegħek għall-komunikazzjoni.

- Websajt
- Email
- Rapporti
- Arkivjar u riċerka

Il-konsulenzi dwar is-sigurtà mqassma minn CSIRT għandhom dejjem isegwu l-istess struttura. Dan iżid il-faċilità biex jinqraw u l-qarrej malajr isib l-informazzjoni kollha rilevanti.

Konsulenza għandha mill-anqas tinkludi l-informazzjoni li ġejja:

Titlu tal-konsulenza ……
Numru ta' referenza …… **Sistemi affettwati** **-** …… **-** …… **OS relatata + verżjoni** …… **Riskju** (Għoli-Medju-Baxx) …… **Impatt/dannu potenzjali** (Għoli-Medju-Baxx) …… **Id's esterni:** (CVE, ID's tal-bullettin dwar il-vulnerabilità) ……
Ħarsa ġenerali tal-vulnerabilità …… **Impatt** …… **Soluzzjoni** …… **Deskrizzjoni (dettalji)** …… **Appendiċi** ……

Fig. 12 Kampjun ta' skema ta' konsulenza

Ara kapitlu *10. Eżerċizzju* għal eżempju komplet ta' konsulenza dwar is-sigurtà.

Kif Timmaniġġja l-Inċidenti

Kif intqal fl-introduzzjoni ta' dan il-kapitlu, il-proċess ta' l-immaniġġar ta' l-informazzjoni waqt il-ġestjoni ta' inċident huwa simili ħafna għal dak użat waqt il-kompilazzjoni ta' allarmi, twissijiet u dikjarazzjonijiet. Iżda l-parti tal-ġbir ta' l-informazzjoni ġeneralment hija differenti, billi l-mod normali ta' kif tinkiseb informazzjoni relatata ma' l-inċidenti huwa jew billi jaslu rapporti ta' l-inċident mill-kostitwenza jew timijiet oħra, jew billi jaslu kummenti minn partijiet involuti waqt il-proċess ta' l-immaniġġar ta' l-inċident. L-informazzjoni ġeneralment tgħaddi permezz ta' e-mail (kodifikata); kultant l-użu tat-telefon jew faks huwa neċessarju.

Meta tirċievi informazzjoni bit-telefon, hija prattika tajba li tniżżel kull dettall partikolari mill-ewwel jew billi tuża strument għall-immaniġġar/rappurtar ta' l-inċident jew billi tagħmel memo. Huwa neċessarju li toħloq immedjatament (qabel ma tintemm it-telefonata) numru ta' l-inċident (jekk ikun għad m'hemmx wieħed għal dan l-inċident) u tagħtih lill-persuna li tkun qiegħda tagħmel ir-rapport bit-telefon (jew b'e-mail ta' sommarju li tintbagħat wara) bħala referenza għal komunikazzjoni sussegwenti.

Il-bqija ta' dan il-kapitlu tiddeskrivi l-proċess bażiku ta' l-immaniġġar ta' inċident. Analiżi dettaljata ħafna tal-proċess sħiħ ta' l-immaniġġjar ta' l-inċidenti u l-flussi tax-xogħol u s-sottoflussi tax-xogħol kollha involuti tista' tinstab fid-dokumentazzjoni *Definizzjoni tal-Proċessi ta' l-Immaniġġar ta' l-Inċidenti għall-CSIRTs* tal-CERT/CC[24].

[24] Definizzjoni tal-Proċessi ta' l-Immaniġġar ta' l-Inċidenti: http://www.cert.org/archive/pdf/04tr015.pdf

Bażikament, l-immaniġġar ta' l-inċidenti jsegwi l-fluss tax-xogħol li ġej:

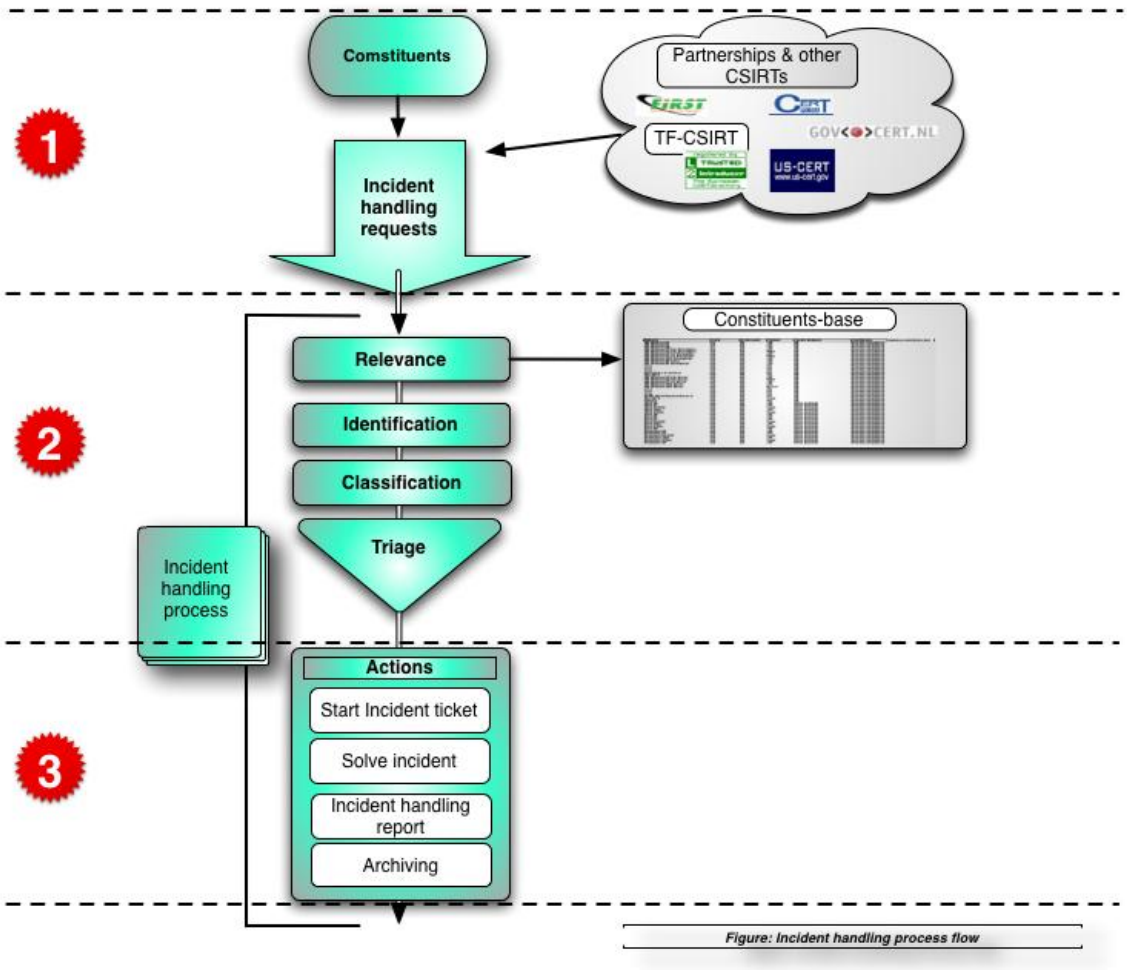


Fig. 13 Kif jimxi l-proċess ta' inċident

Pass 1: Meta tirċievi rapporti ta' inċidenti

Kif issemma qabel, ir-rapporti ta' l-inċidenti jaslu għand CSIRT b'diversi modi, l-aktar b'e-mail iżda anki bit-telefon jew faks.

Kif issemma qabel, hija prattika tajba li tniżżel id-dettalji kollha f'format fiss waqt li tkun qed tirċievi rapport ta' inċident. B'dan jiġi żgurat li ebda informazzjoni importanti ma titħalla barra. Aktar 'il quddiem wieħed jista' jsib skema kampjun:

FORMOLA GĦAR-RAPPURTAR TA' INĊIDENT
Jekk jogħġbok imla din il-formola u ibgħatha b'Faks jew b'email lil: …….. *Il-linji mmarkati b'* huma meħtieġa.* *Name and Organisation* 1. Isem*: 2. Isem ta' l-Organizzazzjoni*: 3. Tip ta' settur: 4. Pajjiż*: 5. Belt: 6. Indirizz ta' l-e-mail*: 7. Numru tat-telefon*: 8. Oħrajn: *Ospitant(i) Affettwat(i)* 9. Numru ta' Ospitanti: 10. Isem l-Ospitant u l-IP*: 11. Funzjoni ta' l-Ospitant*: 12. Żona tal-Ħin: 13. Ħardwer: 14. Sistema Operattiva: 15. Softwer Affettwat: 16. Fajls Affettwati: 17. Sigurtà: 18. Isem l-Ospitant u l-IP: 19. Protokoll/port: *Inċident* 20. Numru ta' referenza # ta' ref: 21. Tip ta' inċident: 22. L-inċident Beda: 23. Dan huwa inċident li għadu għaddej: IVA LE 24. Ħin u Metodu ta' l-Iskoperta: 25. Vulnerabilitajiet Magħrufa: 26. Fajls Suspettużi: 27. Kontromiżuri: 28. Deskrizzjoni dettaljata*:

Fig. 14 Kontenut ta' rapport ta' inċident

Pass 2: Evalwazzjoni ta' l-Inċident

F'dan l-istadju tiġi ċċekkjata l-awtentiċità u r-rilevanza ta' inċident irrapportat u l-inċident jiġi kklassifikat.

Identifikazzjoni

Biex tiġi evitata kwalunkwe azzjoni bla bżonn hija drawwa tajba li tiċċekkja jekk l-oriġinatur huwiex affidabbli u jekk l-oriġinatur huwiex wieħed mill-kostitwenti tiegħek jew ta' CSIRTs kollegi. Regoli simili kif deskritti f'kapitlu 8.2 *Produzzjoni ta' Allarmi* japplikaw.

Rilevanza

B'dan il-pass inti tiċċekkja jekk it-talba għall-immaniġġar ta' inċident toriġinax mill-kostitwenza tal-CSIRT, jew jekk l-inċident irrappurtat jinvolvix sistemi ta' l-IT mill-kostitwenza. Jekk l-ebda waħda minn dawn ta' hawn fuq ma tapplika, ir-rapport ġeneralment jiġi dirett mill-ġdid lill-CSIRT korrett[25].

Klassifikazzjoni

B'dan il-pass it-*triage* issir billi tiġi kklassifikata l-gravità ta' l-inċident. Mhux fl-iskop ta' dan id-dokument li nidħlu fid-dettalji dwar il-klassifikazzjoni ta' l-inċidenti. Bidu tajjeb ikun li tuża l-iskema għall-Klassifikazzjoni tal-Każijiet tal-CSIRT (Eżempju ta' CSIRT ta' l-Intrapriża):

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.		

Fig. 15 Skema għall-Klassifikazzjoni ta' l-Inċidenti (sors: FIRST)[26]

[25] Għodod biex tiċċekkja l-identitajiet fil-CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] Klassifikazzjoni tal-Każ ta' CSIRT http://www.first.org/resources/guides/csirt_case_classification.html

Triage

Triage hija sistema użata minn persunal mediku jew ta' l-emerġenza biex jitqassmu riżorsi mediċi limitati meta n-numru ta' feruti li jeħtieġu l-kura jaqbeż ir-riżorsi disponibbli biex titwettaq il-kura, bil-għan li jiġi ttrattat l-akbar numru ta' pazjenti possibbli[27].

Il-CERT/CC jagħti d-deskrizzjoni li ġejja:

Triage hija element essenzjali ta' kwalunkwe kapaċità ta' ġestjoni ta' l-inċidenti, b'mod partikolari għal kwalunkwe CSIRT stabbilit. Triage hija fuq ir-rotta kritika biex jiġi mifhum x'qed jiġi rrappurtat madwar l-organizzazzjoni. Hija sservi bħala l-mezz li bih l-informazzjoni kollha tgħaddi għal ġo punt wieħed ta' kuntatt, u hekk tippermetti veduta mill-intrapriża ta' l-attività li tkun għaddejja u korrelazzjoni komprensiva ta' l-informazzjoni kollha rrappurtata. Triage tippermetti evalwazzjoni inizjali ta' rapport li jidħol u tpoġġih fejn imissu għal aktar immaniġġar. Hija tipprovdi wkoll post biex tinbeda d-dokumentazzjoni inizjali u l-kitba ta' l-informazzjoni ta' rapport jew talba, jekk dan ma jkunx diġà sar fil-proċess tas-Sejbien.

Il-funzjoni tat-triage tipprovdi stampa immedjata ta' l-istatus attwali ta' l-attività kollha rrappurtata – liema rapporti huma miftuħa jew magħluqa, x'azzjonijiet huma pendenti, u kemm ġew riċevuti minn kull tip ta' rapport. Dan il-proċess jista' jgħin biex jiġu identifikati problemi potenzjali tas-sigurtà u jiġi prijoritizzat il-volum tax-xogħol. L-informazzjoni miġbura waqt it-triage tista' wkoll tintuża sabiex jiġu ġġenerati xejriet u statistiċi dwar il-vulnerabilità u l-inċidenti għat-tmexxija għolja[28].

Triage għandha ssir mill-aktar membri b'esperjenza tat-tim, minħabba li teħtieġ ftehim fil-fond ta' l-impatti potenzjali ta' l-inċidenti fuq partijiet speċifiċi tal-kostitwenza u l-kapaċità li tiddeċiedi min huwa l-aktar membru adatt tat-tim biex jieħu ħsieb dak l-inċident.

[27] Triage fil-Wikipedia: http://en.wikipedia.org/wiki/Triage

[28] Definizzjoni tal-Proċessi ta' l-Immaniġġar ta' l-Inċidenti: http://www.cert.org/archive/pdf/04tr015.pdf

Pass 3: Azzjonijiet

Ġeneralment l-inċidenti evalwati għall-urġenza jmorru fi kju tat-talbiet f'għodda ta' ġestjoni ta' l-inċidenti użata minn persuna waħda jew aktar li timmaniġġja l-inċidenti, li bażikament isegwu dawn il-passi.

Jinħoloq biljett ta' l-inċident
In-numru tal-biljett ta' l-inċident għandu mnejn diġà jkun ġie ġġenerat fi stadju preċedenti (per eżempju meta l-inċident ġie rrappurtat bit-telefon). Jekk le, l-ewwel pass ikun li jinħoloq numru bħal dan li jintuża f'kull komunikazzjoni oħra dwar dan l-inċident.

Ċiklu tal-ħajja ta' l-inċident
L-immaniġġar ta' inċident ma jsegwix sensiela ta' passi li finalment iwasslu għal soluzzjoni, iżda pjuttost isegwi ċirku ta' passi li jiġu applikati ripetutament sakemm l-inċident finalment jiġi solvut u l-partijiet kollha involuti jkollhom l-informazzjoni neċessarja. Dan iċ-ċirku, li sikwit issir referenza għalih ukoll bħala ċ-"Ċiklu tal-ħajja ta' l-Inċident", fih il-proċessi li ġejjin:

Analiżi:	Id-dettalji kollha ta' l-inċident irrappurtat jiġu analizzati.
Ksib tal-kuntatti:	Biex tkun tista' tiġi rrappurtata aktar l-informazzjoni relatata ma' l-inċident lill-partijiet kollha involuti, bħal CSIRTs oħra, il-vittmi u probabbli s-sidien ta' sistemi li jista' jkun intużaw ħażin għal attakk.
Għoti ta' assistenza teknika:	Għajnuna lill-vittmi biex jirkupraw malajr mir-riżultati ta' l-inċident u ġbir ta' aktar informazzjoni dwar l-attakk.
Koordinament:	Infurmar lil partijiet oħra involuti bħall-CSIRT responsabbli għas-sistema ta' l-IT użata għal attakk, jew vittmi oħra.

Din l-istruttura tissejjaħ "ċiklu tal-ħajja", minħabba li pass iwassal għall-ieħor u l-aħħar wieħed, il-parti tal-koordinament, tista' mill-ġdid twassal għal analiżi ġdida, u ċ-ċiklu jerġa' jibda. Il-proċess jintemm meta l-partijiet kollha involuti jkunu rċevew u rrappurtaw l-informazzjoni kollha neċessarja.

Jekk jogħġbok irreferi għall-manwal tal-CERT/CC għal deskrizzjoni aktar dettaljata taċ-ċiklu tal-ħajja ta' inċident[29].

Rapport dwar l-immaniġġar ta' l-inċident
Kun lest għal mistoqsijiet mit-tmexxija dwar l-inċidenti billi tħejji rapport. Hija prattika tajba wkoll li tikteb document (għall-użu intern biss) dwar il-"lezzjonijiet mitgħallma" biex tgħallem lill-persunal u biex jiġu evitati l-iżbalji fi proċessi futuri ta' immaniġġar ta' l-inċidenti.

Arkivjar
Ara r-regoli ta' l-arkivjar deskritti aktar kmieni f'kapitlu *6.6 Żvilupp ta' politika dwar is-sigurtà ta' l-informazzjoni*.

Jekk jogħġbok irreferi għall-Anness sezzjoni *A.1 Aktar qari* għal gwidi komprensivi dwar l-immaniġġar ta' l-inċidenti u ċ-ċiklu tal-ħajja ta' l-inċidenti.

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

Eżempju ta' skeda ta' rispons

Id-definizzjoni tal-ħinijiet tar-rispons ħafna drabi tiġi injorata iżda trid tkun parti minn kull ftehim strutturat sewwa dwar il-livell ta' servizz (SLA – *Service Level Agreement*) bejn CSIRT u l-kostitwenza tiegħu. L-għoti ta' kummenti f'waqthom lill-kostitwenti waqt l-immaniġġar ta' inċident hija kruċjali, kemm għar-responsabbiltajiet stess tal-kostitwenti kif ukoll għar-reputazzjoni tat-tim.
Il-ħinijiet tar-rispons iridu jiġu kkomunikati b'mod ċar lill-kostitwenza biex jiġu evitati aspettattivi ħżiena. L-iskeda bażika ħafna li ġejja tista' tintuża bħala punt tal-bidu għal SLA aktar dettaljata ma' kostitwenza tal-CSIRTs.

Dan li ġej huwa eżempju ta' skeda ta' rispons prattika mill-mument ta' talba li tidħol għal assistenza:

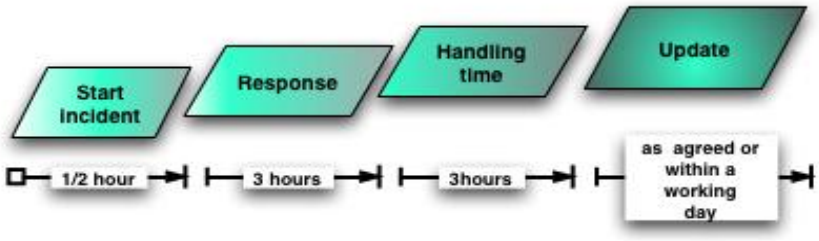


Fig. 16 Eżempju ta' skeda ta' rispons

Hija wkoll prattika tajba li tgħallem lill-kostitwenza dwar il-ħinijiet tar-rispons tagħhom, speċjalment meta għandhom jikkuntattjaw lill-CSIRT f'każ ta' emerġenza. Ħafna drabi huwa aħjar li jikkuntattjaw lill-CSIRT tagħhom fi stadju bikri, u hija prattika tajba li tinkoraġġixxi l-kostitwenza biex tagħmel dan f'każ ta' dubju.

Għodod disponibbli għal CSIRT

Dan il-kapitlu jipprovdi xi referenzi għal għodod komuni użati mill-CSIRTs. Huwa jagħti biss eżempji, aktar indikaturi jistgħu jinstabu fil-*Clearinghouse ta' l-Għodod għall-Immaniġġar ta' l-Inċidenti* [30] (CHIHT).

Email u softwer għall-kodifikar tal-messaġġi

- GNUPG http://www.gnupg.org/
  GnuPG hija l-implimentazzjoni sħiħa u b'xejn ta' l-istandard OpenPGP tal-proġett GNU kif definite mir-RFC2440. GnuPG tippermettilek li tikkodifika u tiffirma l-informazzjoni u l-komunikazzjoni tiegħek.

- PGP http://www.pgp.com/
  Varjant kummerċjali

Għodda għall-immaniġġar ta' l-inċidenti

Timmaniġġja l-inċidenti u l-*follow-up* tagħhom, u b'hekk iżżomm rekord ta' l-azzjonijiet.

- RTIR http://www.bestpractical.com/rtir/
  RTIR hija sistema *open source* mingħajr ħlas għall-immaniġġar ta' l-inċidenti, imfassla skond il-ħtiġijiet tat-timijiet CERT u timijiet oħra ta' rispons għall-inċidenti.

Għodod CRM

Meta jkollok ħafna kostitwenti differenti u tkun trid tintraċċa l-appuntamenti u d-dettalji kollha, database CRM hija utli. Hemm ħafna varjazzjonijiet differenti, dawn huma xi eżempji:

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

- Sugarforce (Verżjoni open source mingħajr ħlas)
  http://www.sugarforge.org/

Iċċekkjar ta' l-informazzjoni

- Għassa tal-websajts
  http://www.aignes.com/index.htm
  Dan il-programm jimmonitorja l-websajts għall-aġġornamenti l-bidliet.

- Ara dik il-paġna http://www.watchthatpage.com/
  Is-servizz jibgħat informazzjoni dwar bidliet fil-websajts permezz ta' email (b'xejn u kummerċjali).

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

Sejba ta' l-informazzjoni ta' kuntatt
Li ssib il-kuntatt korrett biex tirrapporta l-inċidenti mhijiex biċċa xogħol sempliċi. Hemm xi sorsi ta' informazzjoni li jistgħu jintużaw:

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

Barra minn hekk, il-CHIHT jelenka xi għodod sabiex tinstab informazzjoni ta' kuntatt[34].

CSIRT fittizju (pass 8)
Stabbiliment tal-flussi tal-proċess u proċeduri tekniċi u operattivi CSIRT Fittizju jiffoka fuq l-għoti ta' servizzi bażiċi ta' CSIRT: • Allarmi u Twissijiet • Dikjarazzjonijiet • Ġestjoni ta' l-Inċident It-tim żviluppa proċeduri li jaħdmu sewwa u li jinftiehmu mingħajr tbatija minn kull membru tat-tim. CSIRT Fittizju qabbad ukoll espert legali biex jieħu ħsieb ir-responsabbiltajiet u l-politika dwar is-sigurtà ta' l-informazzjoni. It-tim adotta xi għodod utli u sab informazzjoni siewja dwar kwistjonijiet operattivi billi ddiskuta ma' CSIRTs oħra. Saret template fissa għall-konsulenzi dwar is-sigurtà u r-rapporti dwar l-inċidenti. It-tim juża l-RTIR għall-ġestjoni ta' l-inċidenti.

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

[32] IRT-object fid-database tar-RIPE: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Introduttur ta' Fiduċja: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Għodod biex jiġu ċċekkjati l-identitajiet fil-CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Taħriġ tal-CSIRT

Sa issa għamilna l-passi li ġejjin:

1. Ftehim ta' x'inhu CSIRT u x'benefiċċji jista' jipprovdi.
2. Lil liema settur ser jipprovdi s-servizzi tiegħu t-tim il-ġdid?
3. X'tipi ta' servizzi jista' jipprovdi CSIRT lill-kostitwenza tiegħu.
4. Analiżi ta' l-ambjent u l-kostitwenti.
5. Definizzjoni tad-dikjarazzjoni tal-missjoni.
6. Żvilupp tal-Pjan Korporattiv.
   a. Definizzjoni tal-mudell finanzjarju.
   b. Definizzjoni ta' l-istruttura organizzattiva.
   ċ. Bidu ta' tħaddim tal-persunal.
   d. Użu u tagħmir ta' l-uffiċċju.
   e. Żvilupp ta' politika dwar is-sigurtà ta' l-informazzjoni
   f. Tfittxija għal sħab ta' kooperazzjoni.
7. Promozzjoni tal-Pjan Korporattiv.
   a. Approvazzjoni tal-każ korporattiv.
   b. Daħħal kollox fi pjan tal-proġett.
8. Il-CSIRT isir operattiv.
   a. Ħolqien ta' flussi tax-xogħol
   b. Implimentazzjoni ta' għodod tal-CSIRT

>> Il-pass li jmiss huwa: ħarreġ il-persunal

Dan il-kapitlu jsemmi ż-żewġ sorsi prinċipali għal taħriġ iddedikat għall-CSIRT: TRANSITS u l-korsijiet tal-CERT/CC.

TRANSITS

TRANSITS kien proġett Ewropew biex jippromwovi l-istabbiliment ta' Timijiet ta' Rispons għall-Inċidenti ta' Sigurtà tal-Kompjuters (CSIRTs) u t-titjib ta' CSIRTs eżistenti billi jindirizza l-problema tan-nuqqas ta' persunal imħarreġ tal-CSIRTs. Din il-mira ġiet indirizzata billi ġew ipprovduti korsijiet speċjalizzati ta' taħriġ biex il-persunal tal-CSIRTs (il-ġodda) jiġi mħarreġ fil-kwistjonijiet organizzattivi, operattivi, tekniċi, tas-suq u legali involuti fl-għoti tas-servizzi ta' CSIRT.

B'mod partikolari, TRANSITS

- żviluppa, aġġorna u rreveda b'mod regolari materjal modulari tal-korsijiet ta' taħriġ
- organizza *workshops* ta' taħriġ fejn tqassmu l-materjali tal-kors
- ippermetta l-parteċipazzjoni tal-membri tal-persunal ta' CSIRTs (ġodda) f'dawn il-*workshops* ta' taħriġ, b'enfasi partikolari fuq il-parteċipazzjoni mill-Istati tas-Sħubija fl-UE
- qassam il-materjali tal-korsijiet ta' taħriġ u assigura l-użu tar-riżultati[35].

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

ENISA qiegħda tiffaċilita u tappoġġja l-korsijiet ta' TRANSITS. Jekk trid tkun taf kif tapplika għall-korsijiet, ir-rekwiżiti u l-prezzijiet, jekk jogħġbok ikkuntattja lill-esperti dwar il-CSIRT ta' ENISA:

CERT-Relations@enisa.europa.eu

Jekk jogħġbok sib kampjun tal-materjal tal-kors fl-anness ta' dan id-dokument!

CERT/CC

Il-kumplessità ta' l-infrastrutturi tal-kompjuter u tan-netwerk u l-isfida ta' l-amministrazzjoni jagħmluha diffiċli biex timmaniġġja sewwa s-sigurtà tan-netwerk. L-amministraturi tan-netwerk u tas-sistema m'għandhomx biżżejjed nies u prattiċi tas-sigurtà fis-seħħ biex jiddefendu kontra l-attakki u jillimitaw il-ħsara. Minħabba f'hekk l-ammont ta' inċidenti tas-sigurtà tal-kompjuters qiegħed dejjem jiżdied.
Meta jseħħu inċidenti tas-sigurtà tal-kompjuter, l-organizzazzjonijiet iridu jirrispondu malajr u b'mod effettiv. Aktar ma organizzazzjoni tagħraf, tanalizza u tirrispondi malajr għal inċident, aktar tkun tista' tillimita d-dannu u tnaqqas l-ispejjeż ta' l-irkupru. Li tistabbilixxi tim ta' rispons għall-inċidenti tas-sigurtà tal-kompjuters (CSIRT) huwa mod tajjeb ħafna kif tipprovdi din il-kapaċità ta' rispons rapidu kif ukoll biex tevita inċidenti fil-futur.

CERT-CC joffri korsijiet għall-maniġers u l-persunal tekniku f'oqsma bħall-ħolqien u l-immaniġġjar tat-timijiet ta' rispons għall-inċidenti tas-sigurtà tal-kompjuter (CSIRTs), jirrispondi għal u janalizza inċidenti tas-sigurtà, u jtejjeb is-sigurtà tan-netwerk. Sakemm ma jkunx innotat mod ieħor, il-korsijiet kollha jsiru f'Pittsburgh, PA. Il-membri tal-persunal tagħna jgħallmu wkoll korsijiet dwar is-sigurtà f'Carnegie Mellon University.

Korsijiet disponibbli tal-CERT/CC iddedikati għall-CSIRTs[36]

- Kif toħloq Tim ta' Rispons għall-Inċidenti ta' Sigurtà tal-Kompjuter – *Creating a Computer Security Incident Response Team* (CSIRT)
- Kif timmaniġġja t-Timijiet ta' Rispons għall-Inċidenti ta' Sigurtà tal-Kompjuters (CSIRTs) *Managing Computer Security Incident Response Teams* (CSIRTs)
- Fundamentali ta' l-Immaniġġjar ta' l-Inċidenti – *Fundamentals of Incident Handling*
- Immaniġġjar Avanzat ta' l-Inċidenti għall-Persunal Tekniku - *Advanced Incident Handling for Technical Staff*

Jekk jogħġbok sib materjal kampjun tal-kors fl-anness ta' dan id-dokument!

CSIRT Fittizju (pass 9)
Taħriġ tal-persunal CSIRT Fittizju jiddeċiedi li jibgħat il-persunal tekniku kollu tiegħu għall-korsijiet li jmiss ta' TRANSITS. Barra minn hekk il-mexxej tat-tim jattendi l-kors *Kif tmexxi CSIRT* mill-CERT/CC.

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

10 Eżerċizzju: produzzjoni ta' konsulenza

Sa issa għamilna l-passi li ġejjin:

1. Ftehim ta' x'inhu CSIRT u x'benefiċċji jista' jipprovdi.
2. Lil liema settur ser jipprovdi s-servizzi tiegħu t-tim il-ġdid?
3. X'tipi ta' servizzi jista' jipprovdi CSIRT lill-kostitwenza tiegħu.
4. Analiżi ta' l-ambjent u l-kostitwenza.
5. Definizzjoni tad-dikjarazzjoni tal-missjoni.
6. Żvilupp tal-Pjan Koroprattiv.
   a. Definizzjoni tal-mudell finanzjarju.
   b. Definizzjoni ta' l-istruttura organizzattiva.
   ċ. Bidu ta' tħaddim tal-persunal.
   d. Użu u tagħmir ta' l-uffiċċju.
   e. Żvilupp ta' politika dwar is-sigurtà ta' l-informazzjoni
   f. Tfittxija għal sħab ta' kooperazzjoni.
7. Promozzjoni tal-Pjan Korporattiv.
   a. Approvazzjoni tal-każ korporattiv.
   b. Daħħal kollox fi pjan tal-proġett.
8. Il-CSIRT isir operattiv.
   a. Ħolqien ta' flussi tax-xogħol
   b. Implimentazzjoni ta' l-għodod tal-CSIRT
9. Taħriġ tal-persunal tiegħek

>> Il-pass li jmiss huwa li tipprattika u tkun lest għax-xogħol propju!

Bħala eżempju, dan il-kapitlu jiddeskrivi eżempju kampjun għal biċċa xogħol ta' kuljum tal-CSIRT: ħolqien ta' konsulenza dwar is-sigurtà.

L-istimolu kien il-konsulenza oriġinali dwar is-sigurtà mibgħuta minn Microsoft:

Identifikatur tal-Bullettin	**Bullettin tal-Microsoft dwar is-Sigurtà MS06-042**
Titlu tal-Bullettin	**Aġġornament Kumulattiv dwar is-Sigurtà għall-Internet Explorer (918899)**
Sommarju Esekuttiv	Dan l-aġġornament jirrisolvi diversi vulnerabilitajiet fl-Internet Explorer li jistgħu jippermettu esekuzzjoni mill-bogħod tal-kodiċi.
Valutazzjoni ta' l-Akbar Serjetà	Kritika
Impatt tal-Vulnerabilità	Esekuzzjoni mill-Bogħod tal-Kodiċi
Softwer Affettwat	**Windows, Internet Explorer.** Għal aktar informazzjoni, ara t-taqsima dwar is-Softwer Affettwat u l-Postijiet tat-Tniżżil.

Dan il-bullettin tal-bejjiegħ jindirizza vulnerabilità misjuba riċentement fl-Internet Explorer. Il-bejjiegħ jippubblika diversi soluzzjonijiet għal dan is-softwer għal bosta verżjonijiet tal-Windows tal-Microsoft.

CSIRT Fittizju, wara li rċieva din l-informazzjoni dwar il-vulnerabilità permezz ta' lista ta' l-impustar, jibda bil-fluss tax-xogħol deskritt f'kapitlu *8.2 Produzzjoni ta' Allarmi, Twissijiet u Dikjarazzjonijiet*.

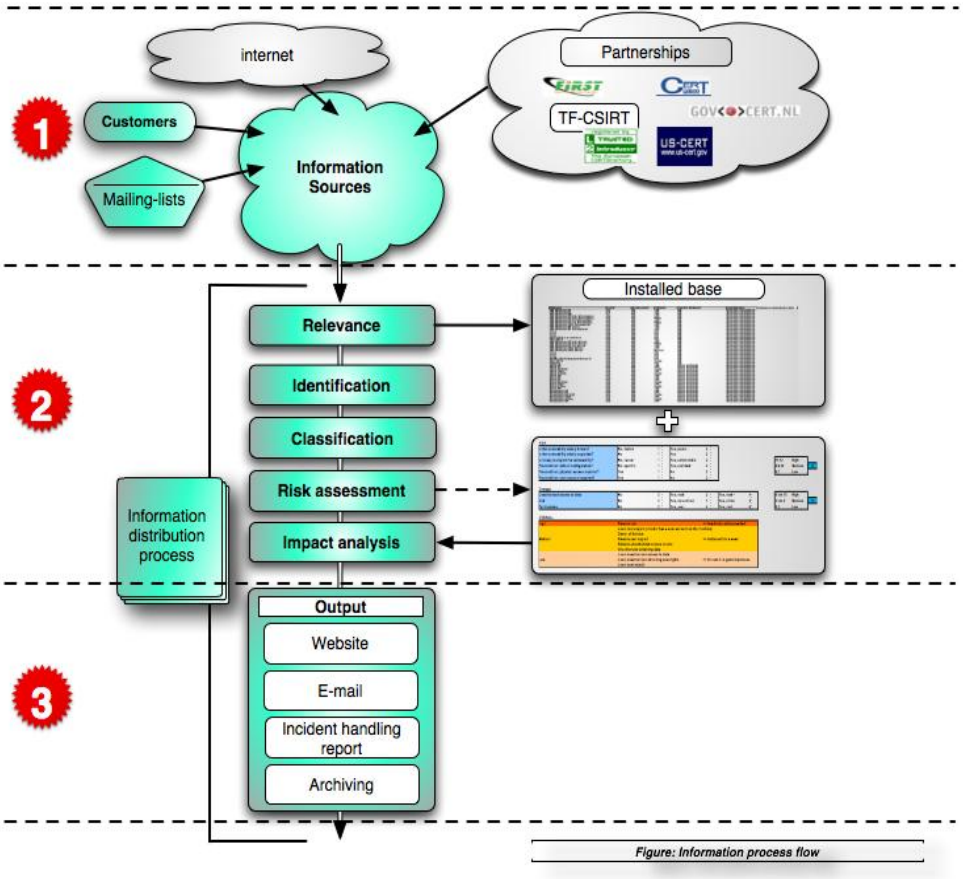


Figure: Information process flow

1 Pass 1: Ġbir ta' informazzjoni dwar il-vulnerabilità.

L-ewwel pass huwa li tibbrawżja l-websajt tal-bejjiegħ. Hemmhekk, CSIRT Fittizju jivverifika l-awtentiċità ta' l-informazzjoni u jiġbor aktar dettalji dwar il-vulnerabilità tas-sistemi ta' l-IT affettwati.

Pass 2: Evalwazzjoni ta' l-informazzjoni u stima tar-riskju

Identifikazzjoni
L-informazzjoni diġà ġiet verifikata billi ġiet iċċekkjata l-informazzjoni dwar il-vulnerabilità riċevuta b'email mat-test fuq il-websajt tal-bejjiegħ.

Rilevanza
CSIRT Fittizju jiċċekkja l-lista tas-sistemi affettwati misjuba fuq il-websajt mal-lista tas-sistemi użati fil-kostitwenza. Huwa jsib li mill-anqas wieħed mill-kostitwenti juża l-Internet Explorer, għalhekk l-informazzjoni dwar il-vulnerabilità hija tassew rilevanti.

	Applikazzjoni	Prodott tas-Softwer	Verżjoni	OS	Verżjoni ta' l-OS	Kostitwent
Desktop	Brawżer	IE	x-x-	Microsoft	XP-prof	A

Klassifikazzjoni
L-informazzjoni hija pubblika u għalhekk tista' tintuża u terġa' titqassam.

Stima tar-riskju u analiżi ta' l-impatt
It-tweġibiet għall-mistoqsijiet juru li r-riskju u l-impatt huma *għolja* (valutati bħala *kritiċi* minn Microsoft).

RISKJU

Il-vulnerabilità magħrufa sewwa?	IVA
Il-vulnerabilità mifruxa?	IVA
Faċli tisfrutta l-vulnerabilità?	IVA
Il-vulnerabilità tista' tiġi sfruttata mill-bogħod?	IVA

ĦSARA
L-impatti possibbli huma aċċessibilità mill-bogħod u potenzjalment esekuzzjoni mill-bogħod tal-kodiċi. Din il-vulnerabilità fiha diversi kwistjonijiet, li jagħmlu r-riskju tal-ħsara *għoli*.

Pass 3: Tqassim

Il-CSIRT Fittizju huwa CSIRT intern. Huwa għandu email, telefon u websajt interna disponibbli bħala kanali ta' komunikazzjoni. Il-CSIRT jipprovdi din il-konsulenza, meħuda mit-template minn kapitlu *8.2 Produzzjoni ta' Allarmi, Twissijiet u Dikjarazzjonijiet*.

Titlu tal-konsulenza
Diversi vulnerabilitajiet misjuba fl-Internet explorer

Numru ta' referenza
082006-1

Sistemi affettwati

- Is-sistemi kollha tad-desktop li jaħdmu bil-Microsoft

OS relatata + verżjoni

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 u Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional Edizzjoni x64
- Microsoft Windows Server 2003 u Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 għal Sistemi bbażati fuq l-Itanium u Microsoft Windows Server 2003 bl-SP1 għal Sistemi bbażati fuq l-Itanium
- Microsoft Windows Server 2003 Edizzjoni x64

Riskju (Għoli-Medju-Baxx)
GĦOLI

Impatt/dannu potenzjali (Għoli-Medju-Baxx)
GĦOLI

Id's esterni: (CVE, ID's tal-Bullettin dwar il-vulnerabilità)
MS-06-42

Ħarsa ġenerali tal-vulnerabilità
Microsoft sabet diversi vulnerabilitajiet kritiċi fl-Internet Explorer li wkoll jistgħu jwasslu għal esekuzzjoni mill-bogħod tal-kodiċi.

Impatt
Aggressur jista' jieħu kontroll sħiħ tas-sistema, jinstalla programm, iżid utenti u jikkompeti, jibdel jew ineħħi informazzjoni. Fattur ta' mitigazzjoni huwa li dan ta' hawn fuq jista' jseħħ biss jekk l-utent ikun illoggjat bi drittijiet ta' l-amministratur. Utenti lloggjati b'anqas drittijiet jistgħu jiġi affettwati anqas.

Soluzzjoni
Irranġa l-IE tiegħek immedjatament

Deskrizzjoni (dettalji)
Għal aktar informazzjoni ara ms06-042.mspx

Appendiċi
Għal aktar informazzjoni ara ms06-042.mspx

Dan il-prodott issa huwa lest biex jitqassam. Minħabba li huwa bullettin kritiku, huwa rakkomandat li jissejħu wkoll il-kostitwenti meta jkun possibbli.

CSIRT Fittizju (pass 10)
Eżerċizzju Matul l-ewwel ġimgħat ta' l-operazzjonijiet, il-CSIRT fittizju uża diversi każijiet fittizji (li huma kisbu bħala eżempji minn CSIRTs oħra) li ntużaw bħala eżerċizzju. Barra minn hekk huma ħarġu għadd ta' konsulenzi dwar is-sigurtà bbażati fuq tagħrif reali dwar il-vulnerabilità mqassam minn bejjiegħa tal-ħardwer u tas-softwer, li huma adattaw u aġġustaw għall-ħtiġijiet tal-kostitwenza.

11 Konklużjoni

Hawnhekk tintemm il-gwida. Dan id-dokument huwa maħsub sabiex jagħti ħarsa ġenerali konċiża ħafna tad-diversi proċessi meħtieġa sabiex jitwaqqaf CSIRT. Hija ma tippretendix li tkun kompleta u lanqas ma tidħol iżżejjed f'dettalji speċifiċi. Jekk jogħġbok irreferi għat-taqsima *A.1 Aktar qari* fl-anness għal letteratura dwar dak is-suġġett li ta' min jaqraha.

Il-passi importanti li jmiss għall-CSIRT Fittizju issa jkunu:

- Li jirċievi kummenti mill-kostitwenza biex jipperfezzjona s-servizzi pprovduti
- Li jikseb rutina fix-xogħol ta' kuljum
- Li jeżerċita f'sitwazzjonijiet ta' emerġenza
- Li jibqa' f'kuntatt mill-qrib mad-diversi komunitajiet CSIRT bil-għan li xi darba jikkontribwixxi għax-xogħol volontarju tagħhom

12 Deskrizzjoni tal-Pjan tal-Proġett

NOTA: Il-pjan tal-proġett huwa stima inizjali taż-żmien meħtieġ. Jiddependi fuq ir-riżorsi disponibbli, it-tul real ital-proġett jista' jkun differenti.

Il-pjan tal-proġett huwa disponibbli f'formati differenti fuq CD u l-websejt ta' l-ENISA. Huwa jkopri kompletament il-proċess kollha deskritti f'dan id-dokument.

Il-format prinċipali se jkun il-Microsoft Project, għalhekk jista' jintuża direttament f'din l-għodda ta' ġestjoni tal-proġett.

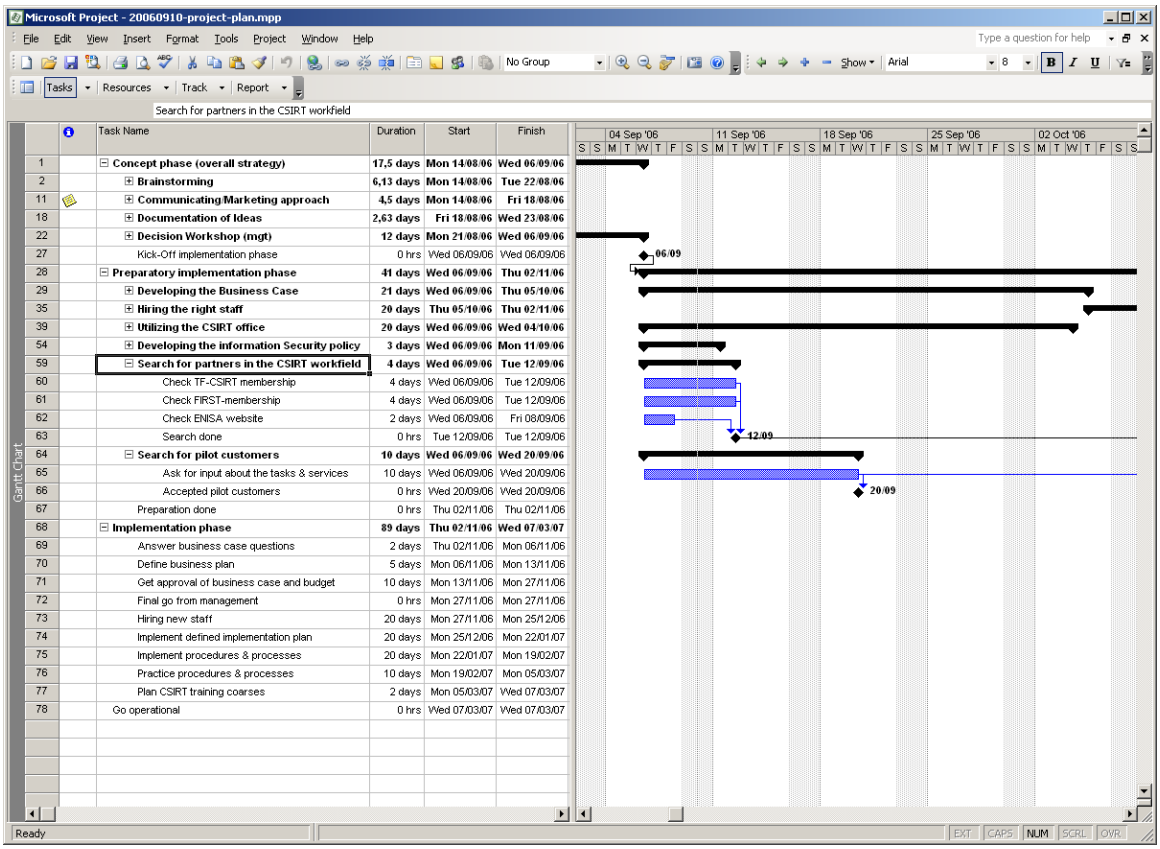
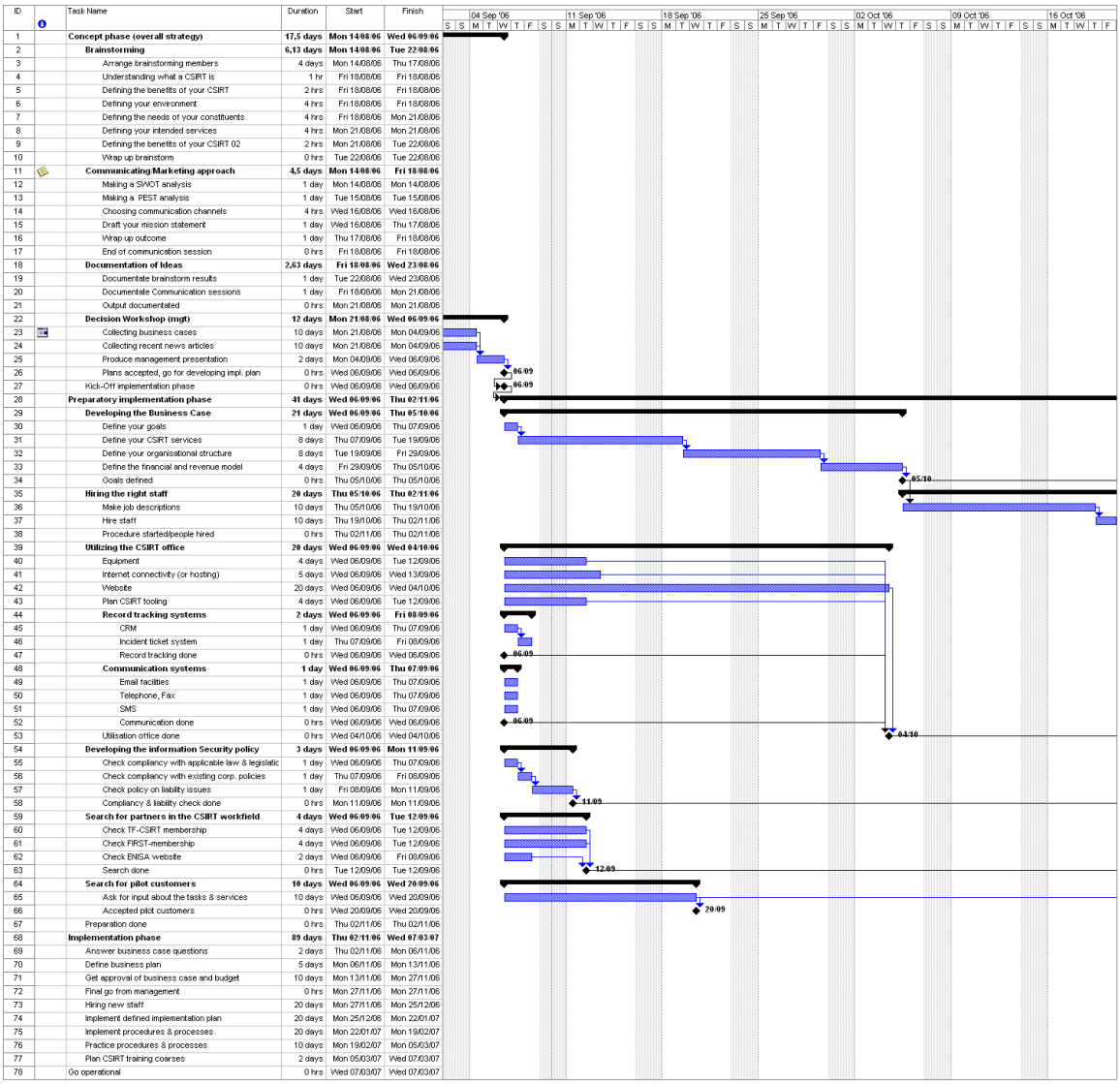


Fig. 17 Pjan tal-proġett



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 courses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Fig. 18 Il-pjan tal-proġett bix-xogħlijiet kollha u parti mill-Gant chart

Il-pjan tal-proġett huwa disponibbli wkoll f'format CVS u XML. Aktar użu jista' jintalab mill-esperti dwar il-CSIRT ta' l-ENISA: CERT-Relations@enisa.europa.eu

APPENDIĊI

A.1 Aktar qari

Handbook for CSIRTs (CERT/CC)
Xogħol ta' referenza tassew komprensiv dwar is-suġġetti kollha rilevanti għall-ħidma ta' CSIRT
Sors: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress
Analiżi dettaljata ta' l-immaniġġjar ta' l-inċidenti
Sors: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs)
Analiżi komprensiva tas-sitwazzjoni attwali fir-rigward tax-xenarju tal-CSIRTs madwar id-dinja, li tinkludi storja, statistiċi u ħafna aktar
Sors: http://www.cert.org/archive/pdf/03tr001.pdf

CERT -in-a-box
Deskrizzjoni komprensiva tal-lezzjonijiet meħuda mit-twaqqif tal-GOVCERT.NL u d-'De Waarschuwingsdienst', is-servizz ta' Twissija nazzjonali Olandiż.
Sors: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response
Sors: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide
Sors: http://www.securityunit.com/publications/sp800-61.pdf

ENISA Inventory of CERT activities in Europe
Xogħol ta' referenza li jagħti informazzjoni dwar il-CSIRTs fl-Ewropa u d-diversi attivitajiet tagħhom
Sors: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: Istitut Nazzjonali ta' l-Istandards u t-Teknoloġiji

Servizzi ta' CSIRT

Ringrazzjament speċjali lill-CERT/CC, li pprovdew din il-lista

Servizzi Reattivi	**Servizzi Proattivi**	**Immaniġġar ta' l-Artefatt**
• Allarmi u Twissijiet • Immaniġġar ta' Inċident • Analiżi ta' Inċident • Rispons għall-inċident fuq il-post • Appoġġ b'Rispons għal Inċident • Koordinament tar-Rispons għal Inċident • Rispons għall-Inċident fuq il-post • Immaniġġar tal-Vulnerabilità • Analiżi tal-Vulnerabilità • Rispons għall-vulnerabilità • Koordinament tar-rispons għall-vulnerabilità	• Dikjarazzjonijiet • Għassa għat-Teknoloġija • Verifiki u Evalwazzjonijiet tas-Sigurtà • Konfigurazzjoni u Manutenzjoni tas-Sigurtà • Żvilupp ta' Għodod tas-Sigurtà • Servizzi għas-Sejbien ta' Intrużjoni • Tixrid ta' Informazzjoni Relatata mas-Sigurtà	• *Analiżi ta' l-artefatt* • *Rispons għall-artefatt* • *Koordinament tar-rispons għall-artefatt* ***Ġestjoni tal-Kwalità tas-Sigurtà*** • *Analiżi tar-Riskju* • *Kontinwità tan-Negozju u Irkupru minn Diżastru* • *Konsulenza dwar is-Sigurtà* • *Tkabbir ta' l-Għarfien* • *Edukazzjoni/Taħriġ* • *Evalwazzjoni jew Ċertifikazzjoni tal-Prodott*

Fig. 19 Lista ta' Servizzi ta' CSIRT mill-CERT/CC

Deskrizzjonijiet tas-Servizzi

Servizzi Reattivi

Is-servizzi reattivi huma mfassla biex jirrispondu għal talbiet għall-assistenza, rapporti ta' inċidenti mill-kostitwenza tal-CSIRT, u kwalunkwe theddidiet jew attakki kontra s-sistemi tal-CSIRT. Xi servizzi jistgħu jinbdew b'avviż minn parti terza jew billi wieħed jara l-monitoraġġ jew l-IDS logs u l-allarmi.

Allarmi u Twissijiet

Dan is-servizz jinvolvi t-tixrid ta' informazzjoni li tiddeskrivi attakk minn intruż, il-vulnerabilità tas-sigurtà, alarm ta' intrużjoni, vajrus tal-kompjuter, jew taqriq, u jipprovdi kwalunkwe kors ta' azzjoni rakkomandat għal żmien qasir biex tiġi indirizzata l-problema li tirriżulta. L-allarm, twissija, jew konsulenza jintbagħtu bħala reazzjoni għall-problema kurrenti biex il-kostitwenti jiġu infurmati bl-attività u biex tingħata gwida dwar kif jipproteġu s-sistemi tagħhom jew jirkupraw kwalunkwe sistemi li ġew affettwati. L-informazzjoni tista' tinħoloq mill-CSIRT jew tista' terġa' titqassam mill-bejjiegħa, CSIRTs oħra jew esperti tas-sigurtà, jew partijiet oħra tal-kostitwenza.

Immaniġġar ta' l-Inċidenti

L-immaniġġar ta' l-inċidenti jinvolvi r-riċeviment, l-analiżi ta' l-urġenza u tweġib għat-talbiet u r-rapporti, u analiżi ta' l-inċidenti u avvenimenti. Attivitajiet partikolari ta' rispons jistgħu jinkludu:

- li tieħu azzjoni biex tipproteġi sistemi u netwerks affettwati jew mhedda minn attività ta' intrużjoni
- li tipprovdi soluzzjonijiet u strateġiji ta' mitigazzjoni minn konsulenzi jew allarmi rilevanti
- li tfittex għal attività ta' intrużjoni fuq partijiet oħra tan-netwerk
- li tiffiltra t-traffiku tan-netwerk
- li tibni sistemi mill-ġdid
- li tirrestawra jew issewwi sistemi
- li tiżviluppa strateġiji oħra ta' rispons jew soluzzjonijiet temporanji

Billi l-attivitajiet ta' ġestjoni ta' l-inċident huma implimentati f'diversi modi minn tipi differenti ta' CSIRTs, dan is-servizz huwa kklassifikat aktar skond it-tip ta' attivitajiet imwettqa u t-tip ta' assistenza mogħtija kif ġej:

Analiżi ta' l-Inċident

Hemm ħafna livelli ta' analiżi ta' l-inċident u ħafna sottoservizzi. Bażikament, analiżi ta' l-inċident hija eżami ta' l-informazzjoni u l-evidenza jew artefatti ta' sostenn kollha disponibbli relatati ma' inċident jew episodju. L-għan ta' l-analiżi huwa li jiġi identifikat l-iskop ta' l-inċident, il-miżura tal-ħsara kkawżata mill-inċident, u l-istrateġiji ta' rispons jew soluzzjonijiet temporanji disponibbli. Il-CSIRT jista' juża r-riżultati ta' l-analiżi tal-vulnerabilità u ta' l-artefatt (deskritta taħt) biex jifhem u jipprovdi l-aktar analiżi kompleta u aġġornata ta' dak li seħħ fuq sistema speċifika. Il-CSIRT jikkorrelata l-attività bejn l-inċidenti biex jistabbilixxi kwalunkwe interrelazzjonijiet, xejriet, mudelli, jew firem ta' l-intruż. Żewġ sottoservizzi li jistgħu jsiru bħala parti minn analiżi ta' l-inċident, jiddependi fuq il-missjoni, il-miri u l-proċessi tal-CSIRT, huma

Ġbir ta' evidenza forensika

Il-ġbir, preservazzjoni, dokumentazzjoni, u analiżi ta' l-evidenza minn sistema tal-kompjuter kompromessa biex jiġu determinati l-bidliet fis-sistema u biex jassistu fir-rikostruzzjoni ta' l-avvenimenti li wasslu għall-periklu. Dan il-ġbir ta' informazzjoni jrid isir b'mod li d-dokumenti jipprovdu katina ta' kustodja attestabbli li tkun ammissibbli f'qorti skond ir-regoli ta' l-evidenza. Ix-xogħlijiet involuti fil-ġbir ta' l-evidenza forensika jinkludu (iżda mhumiex limitati għal)l-produzzjoni ta' kopja *bit-image* tal-*hard drive* tas-sistema affettwata; l-iċċekkjar għal bidliet fis-sistema bħal programmi, fajls, servizzi, u utenti ġodda; spezzjoni tal-proċessi funzjonali u ports miftuħin; u l-iċċekkjar għal programmi u *toolkits* ta' *Trojan horse*. Il-persunal tal-CSIRT li jwettaq din il-funzjoni jista' jkollu jkun lest ukoll li jservi bħala xhieda esperta fi proċedimenti tal-qorti.

Insegwiment jew traċċar

It-traċċar ta' l-oriġini ta' l-intruż jew l-identifikazzjoni tas-sistemi li għalihom l-intruż kellu aċċess. Din l-attività tista' tinvolvi l-insegwiment jew traċċar ta' kif l-intruż daħal fis-sistemi affettwati u n-netwerks relatati, liema sistemi ntużaw biex jinkiseb dak l-aċċess, fejn oriġina l-attakk, u x'sistemi u netwerks oħra ntużaw bħala parti mill-attakk. Tista' tinvolvi wkoll tentattiv biex tiġi stabbilita l-identità ta' l-intruż. Dan ix-xogħol jista' jsir mill-CSIRT waħdu iżda ġeneralment jinvolvi ħidma ma' persunal għall-infurzar tal-liġi, fornituri tas-servizz ta' l-Internet, jew organizzazzjonijiet oħra involuti.

Rispons għal inċident fuq il-post

Il-CSIRT jipprovdi assistenza diretta, fuq il-post, biex jgħin lill-kostitwenti jirkupraw minn inċident. Il-CSIRT innifsu janalizza fiżikament is-sistemi affettwati u jagħmel it-tiswija u l-irkupru tas-sistemi, minflok ma jipprovdi biss appoġġ tar-rispons għall-inċident bit-telefon jew bl-email (ara taħt). Dan is-servizz jinvolvi l-azzjonijiet kollha meħuda fuq livell lokali li huma neċessarji jekk jiġi suspettat jew iseħħ inċident. Jekk il-CSIRT ma jkunx fis-sit affettwat, membri tat-tim imorru fis-sit u jwettqu r-rispons. F'każijiet oħra jista' jkun hemm diġà tim lokali fil-post, li jipprovdi rispons għall-inċident bħala parti mix-xogħol ta' rutina tiegħu. Dan huwa partikolarment il-każ jekk l-immaniġġar ta' l-inċident jiġi pprovdut bħala parti mill-funzjoni normali tax-xogħol ta' l-amministraturi ta' sistema, netwerk jew tas-sigurtà minflok CSIRT stabbilit.

Appoġġ tar-rispons għall-inċidenti

Il-CSIRT jassisti u jiggwida lill-vittma(i) ta' l-attakk biex jirkupraw minn inċident permezz tat-telefon, email, faks, jew dokumentazzjoni. Dan jista' jinkludi assistenza teknika fl-interpretazzjoni ta' l-informazzjoni miġbura, forniment ta' informazzjoni ta' kuntatt, jew għoti ta' gwida dwar strateġiji ta' mitigazzjoni u rkupru. Ma jinvolvix azzjonijiet ta' rispons diretti fuq il-post kif deskritt fuq. Minflok, il-CSIRT jipprovdi gwida mill-bogħod biex hekk il-persunal tal-post ikunu jistgħu jwettqu l-irkupru huma stess.

Koordinament tar-rispons għall-inċidenti

Il-CSIRT jikkoordina l-isforz ta' rispons bejn il-partijiet involuti fl-inċident. Dan normalment jinkludi l-vittma ta' l-attakk, siti oħra involuti fl-attakk, u kwalunkwe siti li jkunu jeħtieġu assitenza fl-analiżi ta' l-attakk. Jista' jinkludi wkoll il-partijiet li jipprovdu appoġġ ta' l-IT lill-vittma, bħall-forniturі tas-servizz ta' l-Internet, CSIRTs oħra, u amministraturi tas-sistema u tan-netwerk fuq il-post. Ix-xogħol ta' koordinazzjoni jista' jinkludi ġbir ta' informazzjoni ta' kuntatt, infurmar ta' siti dwar l-involviment potenzjali tagħhom (bħala vittmi jew sors ta' attakk), ġbir ta' statistiċi dwar in-numru ta' siti involuti, u faċilitar ta' l-iskambju u analiżi ta' l-informazzjoni. Parti mix-xogħol ta' koordinazzjoni tista' tinvolvi avviżi u kollaborazzjoni mad-dipartimenti tal-parir legali, riżorsi umani jew relazzjonijiet pubbliċi ta' kumpanija. Ikun jinvolvi wkoll koordinament ma' l-infurzar tal-liġi. Dan is-servizz ma jinvolvix rispons dirett għall-inċident, fuq il-post.

Immaniġġar tal-vulnerabilità

L-immaniġġar tal-vulnerabilità jinvolvi r-riċeviment ta' informazzjoni u rapporti dwar il-vulnerabilitajiet tal-ħardwer u tas-softwer; analiżi tan-natura, il-mekkanika, u l-effetti tal-vulnerabilitajiet; u żvilupp ta' strateġiji ta' rispons sabiex jinstabu u jissewwew il-vulnerabilitajiet. Billi l-attivitajiet għall-immaniġġar tal-vulnerabilità huma implimentati b'diversi modi minn tipi differenti ta' CSIRTs, dan is-servizz huwa kklassifikat aktar skond it-tip ta' attivitajiet imwettqa u t-tip ta' assistenza mogħtija kif ġej:

Analiżi tal-vulnerabilità

Il-CSIRT iwettaq analiżi teknika u eżami tal-vulnerabilitajiet fil-ħardwer u s-softwer. Din tinkludi l-verifika ta' vulnerabilitajiet suspettati u l-eżami tekniku tal-vulnerabilità fil-ħardwer jew is-softwer biex jiġi stabbilit fejn qiegħda u kif tista' tiġi sfruttata. L-analiżi tista' tinkludi reviżjoni tal-kodiċi tas-sors, bl-użu ta' debugger biex jiġi stabbilit fejn isseħħ il-vulnerabilità, jew tentattiv biex tiġi riprodotta l-problema fuq sistema ta' l-ittestjar

Rispons għall-vulnerabilità

Dan is-servizz jinvolvi l-għażla tar-rispons xieraq sabiex tittaffa jew tissewwa l-vulnerabilità. Dan jista' jinvolvi l-iżvilupp jew riċerka ta' soluzzjonijiet, tiswijiet, u soluzzjonijiet temporanji. Jinvolvi wkoll li ħaddieħor jiġi infurmat bl-istrateġija ta' mitigazzjoni, possibbilment billi jinħolqu u jitqassmu konsulenzi jew allarmi. Dan is-servizz jista' jinkludi t-twettiq tar-rispons billi jiġu installati traqqigħ, tiswijiet, jew soluzzjonijiet temporanji.

Koordinament tar-rispons għall-vulnerabilità

Il-CSIRT jgħarraf lid-diversi partijiet ta' l-intrapriża jew il-kostitwenza dwar il-vulnerabilità u jaqsam informazzjoni dwar kif tissewwa jew titnaqqas il-vulnerabilità. Il-CSIRT jivverifika li l-istrateġija ta' rispons għall-vulnerabilità ġiet implimentata b'suċċess. Dan is-servizz jista' jinvolvi komunikazzjoni ma' bejjiegħa, CSIRTs oħra, esperti tekniċi, membri kostitwenti, u l-individwi jew gruppi li fil-bidu skoprew jew irrappurtaw il-vulnerabilità. L-attivitajiet jinkludu faċilitar ta' l-analiżi ta' vulnerabilità jew rapport ta' vulnerabilità; koordinament ta' l-iskedi tal-ħruġ ta' dokumenti korrispondenti, soluzzjonijiet, jew soluzzjonijiet temporanji; u sintetizzar ta' l-analiżi teknika magħmula minn partijiet differenti. Dan is-servizz jista' jinkludi wkoll iż-żamma ta' arkivju jew bażi ta' għarfien pubbliku jew privat ta' informazzjoni dwar il-vulnerabilità u l-istrateġiji ta' rispons korrispondenti.

Immaniġġar ta' l-Artefatt

Artefatt huwa kwalunkwe fajl jew oġġett misjub fuq sistema li jista' jkun involut fit-tfittix jew attakk ta' sistemi u netwerks jew li jkun qiegħed jintuża biex jegħleb miżuri tas-sigurtà. L-artefatti jistgħu jinkludu iżda mhumiex limitati għal vajrusijiet tal-kompjuter, programmi *Trojan horses*, *worms*, *exploit scripts*, u *toolkits*.
L-immaniġġar ta' l-artefatti jinvolvi r-riċeviment ta' informazzjoni dwar u kopji ta' artefatti li jkunu qegħdin jintużaw f'attakki ta' intrużjoni, esplorazzjoni, u kwalunkwe attivitajiet oħra mhux awtorizzati jew ta' disturb. Ladarba jkun riċevut, l-artefatt jiġi eżaminat. Dan jinkludi analiżi tan-natura, il-mekkanika, il-verżjoni u l-użu ta' l-artefatti; u l-iżvilupp (jew suġġeriment) ta' strateġiji ta' rispons għar-rilevament, tneħħija, u protezzjoni kontra dawn l-artefatti. Billi l-attivitajiet għall-immaniġġar ta' l-artefatti huma implimentati b'diversi modi minn tipi differenti ta' CSIRTs, dan is-servizz huwa kklassifikat aktar skond it-tip ta' attivitajiet imwettqa u t-tip ta' assistenza mogħtija kif ġej:

Analiżi ta' l-artefatt

Il-CSIRT iwettaq eżami u analiżi teknika ta' kwalunkwe artefatt misjub fuq sistema. L-analiżi magħmula tista' tinkludi l-identifikazzjoni tat-tip ta' fajl u l-istruttura ta' l-artefatt, it-tqabbil ta' artefatt ġdid ma' artefatti eżistenti jew verżjonijiet oħra ta' l-istess artefatt biex jinstabu similaritajiet u differenzi, jew inġinerija bil-maqlub jew kodiċi ta' l-iżmuntar biex jiġu stabbiliti l-għan u l-funzjoni ta' l-artefatt.

Rispons għall-artefatt

Dan is-servizz jinvolvi l-għażla ta' l-azzjonijiet xierqa biex jinstabu u jitneħħew l-artefatti minn sistema, kif ukoll azzjonijiet biex jimpedixxu l-artefatti milli jiġu installati. Dan jista' jinvolvi l-ħolqien ta' firem li jistgħu jiġu miżjuda ma' softwer kontra l-vajrusijiet jew IDS.

Koordinament tar-rispons għall-artefatti

Dan is-servizz jinvolvi qsim u sintetizzar tar-riżultati ta' l-analiżi u l-istrateġiji ta' rispons relatati ma' artefatt ma' riċerkaturi oħra, CSIRTs, bejjiegħa, u esperti oħra tas-sigurtà. L-attivitajiet jinkludu l-infurmar ta' ħaddieħor u s-sintetizzar ta' l-analiżi teknika minn varjetà ta' sorsi. L-attivitajiet jistgħu jinkludu wkoll iż-żamma ta' arkivju pubbliku jew kostitwent ta' l-artefatti magħrufa u l-impatt tagħhom u l-istrateġiji ta' rispons korrispondenti.

Servizzi Proattivi

Is-servizzi proattivi huma mfassla biex itejbu l-infrastruttura u l-proċessi tas-sigurtà tal-kostitwenza qabel ma jseħħ jew jinstab xi inċident jew episodju. Il-miri prinċipali huma li jiġu evitati l-inċidenti u li jitnaqqas l-impatt u l-iskala tagħhom meta jseħħu.

Dikjarazzjonijiet

Dan jinkludi, iżda mhuwiex limitat għal, allarmi ta' intrużjoni, twissijiet dwar vulnerabilità, u konsulenzi dwar is-sigurtà. Dawn id-dikjarazzjonijiet jinfurmaw lill-kostitwenti dwar żviluppi ġodda fl-impatt fuq perjodu medju jew twil, bħal vulnerabilitajiet jew għodod ta' intrużjoni misjuba ġodda. Id-dikjarazzjonijiet jippermettu lill-kostitwenti li jipproteġu s-sistemi u n-netwerks tagħhom kontra problemi misjuba ġodda qabel ma dawn ikunu jistgħu jiġu sfruttati.

Għassa għat-Teknoloġija

Il-CSIRT jimmonitorja u josserva żviluppi tekniċi ġodda, attivitajiet ta' intrużjoni, u xejriet relatati biex jgħin fl-identifikazzjoni ta' theddidiet futuri. Is-suġġetti riveduti jistgħu jiġu estiżi biex jinkludu deċiżjonijiet legali u leġislattivi, theddidiet soċjali jew politiċi, u teknoloġiji emerġenti. Dan is-servizz jinvolvi qari ta' listi ta' l-impustar dwar is-sigurtà, websajts dwar is-sigurtà, u aħbarijiet kurrenti u artikli fil-ġurnali fl-oqsma tax-xjenza, it-teknoloġija, il-politika, u l-gvern biex tiġi misluta informazzjoni rilevanti għas-sigurtà tas-sistemi u n-netwerks tal-kostitwenti. Dan jista' jinkludi komunikazzjoni ma' partijiet oħra li huma awtoritajiet f'dawn l-oqsma biex jiġi żgurat li tinkiseb l-aħjar u l-aktar informazzjoni jew interpretazzjoni preċiża. Ir-riżultat ta' dan is-servizz jista' jkun xi tip ta' dikjarazzjoni, linji gwida, jew rakkomandazzjonijiet iffokati aktar fuq kwistjonijiet ta' sigurtà fuq perjodu medju għal twil.

Verifiki jew Evalwazzjonijiet tas-Sigurtà

Dan is-servizz jipprovdi evalwazzjoni u analiżi dettaljata ta' l-infrastruttura tas-sigurtà ta' organizzazzjoni, ibbażata fuq ir-rekwiżiti definiti mill-organizzazzjoni jew minn standards oħra ta' l-industrija li japplikaw. Jista' jinvolvi wkoll evalwazzjoni tal-prattiċi tas-sigurtà ta' l-organizzazzjoni. Hemm ħafna tipi ta' verifiki jew evalwazzjonijiet li jistgħu jiġu pprovduti, fosthom

Evalwazzjoni ta' l-infrastruttura

Eżami manwali tal-konfigurazzjonijiet tal-ħardwer u s-softwer, tar-*routers*, il-*firewalls*, is-servers u l-istrumenti tad-*desktop* biex ikun żgurat li dawn jaqblu ma' l-aħjar politiċi dwar is-sigurtà u l-konfigurazzjonijiet standard ta' l-organizzazzjoni jew industrija.

Evalwazzjoni ta' l-aħjar prattika

Intervistar ta' l-impjegati u l-amministraturi tas-sistema u n-netwerk biex jiġi stabbilit jekk il-prattiċi tas-sigurtà tagħhom jaqblux mal-politika definita ta' l-organizzazzjoni dwar is-sigurtà jew xi standards speċifiċi ta' l-industrija.

Skannjar

Użu ta' skanners tal-vulnerabilità u tal-vajrusijiet biex jiġi stabbilit liema sistemi u netwerks huma vulnerabbli.

Ittestjar tal-penetrazzjoni

Ittestjar tas-sigurtà ta' sit billi intenzjonalment jiġu attakkati s-sistemi u n-netwerks tiegħu. Hija meħtieġa l-approvazzjoni tat-tmexxija għolja qabel ma jitwettqu verifiki jew evalwazzjonijiet bħal dawn. Xi wħud minn dawn l-approċċi jistgħu jkunu pprojbiti mill-politika organizzattiva. L-għoti ta' dan is-servizz jista' jinkludi l-iżvilupp ta' sett komuni ta' prattiċi li kontriehom isiru t-testijiet u l-evalwazzjonijiet, flimkien ma' l-iżvilupp ta' sett ta' ħiliet jew rekwiżiti ta' ċertifikazzjoni għall-persunal li jwettaq it-testijiet, l-evalwazzjonijiet, il-verifiki, jew l-eżamijiet. Dan is-servizz jista' jingħata wkoll b'kuntratt lil kuntrattur parti terza jew lil fornitur ta' servizz tas-sigurtà ġestit bil-kompetenza neċessarja fit-twettiq ta' verifiki u evalwazzjonijiet.

Konfigurazzjoni u Manutenzjoni ta' Għodod tas-Sigurtà, Applikazzjonijiet, Infrastrutturi u Servizzi

Dan is-servizz jidentifika jew jipprovdi gwida xierqa dwar kif tikkonfigura u żżomm b'mod sigur l-għodod, l-applikazzjonijiet u l-infrastruttura ġenerali tal-kompjuters użati mill-kostitwenza tal-CSIRT jew mill-CSIRT innifsu. Minbarra li jipprovdi gwida, il-CSIRT jista' jwettaq aġġornamenti tal-konfigurazzjoni u manutenzjoni ta' l-għodod tas-sigurtà u servizzi, bħal IDS, skannjar tan-netwerk jew sistemi ta' monitoraġġ, filters, wrappers, firewalls, netwerks virtwali privati (VPN – virtual private networks), jew mekkaniżmi ta' verifika. Il-CSIRT jista' saħansitra jipprovdi dawn is-servizzi bħala parti mill-funzjoni prinċipali tiegħu. Il-CSIRT jista' wkoll jikkonfigura u jżomm servers, desktops, laptops, assistenti diġitali personali (PDAs), u apparat ieħor bla fil (wireless) skond il-linji gwida tas-sigurtà. Dan is-servizz jinkludi li jittellgħu quddiem it-tmexxija kwalunkwe kwistjonijiet jew problemi bil-konfigurazzjonijiet jew l-użu ta' għodod u applikazzjonijiet li l-CSIRT iħoss li jistgħu jħallu sistema vulnerabbli għal attakk.

Żvilupp ta' Għodod tas-Sigurtà

Dan is-servizz jinkludi l-iżvilupp ta' kwalunkwe għodod ġodda, speċifiċi għall-kostitwenza, li huma meħtieġa jew mixtieqa mill-kostitwenza jew mill-CSIRT innifsu. Dan jista' jinkludi, per eżempju, l-iżvilupp ta' soluzzjonijiet tas-sigurtà għal softwer personalizzat użat mill-kostitwenza jew it-tqassim ta' softwer protett li jista' jintuża biex jinbnew mill-ġdid *hosts* kompromessi. Jista' jinkludi wkoll l-iżvilupp ta' għodod jew *scripts* li jestendu l-funzjonalità ta' għodod tas-sigurtà eżistenti, bħal *plug-in* ġdid għal vulnerabilità jew skanner tan-netwerk, scripts li jiffaċilitaw l-użu ta' teknoloġija tal-kodifikar, jew mekkaniżmi awtomatizzati għat-tqassim ta' soluzzjonijiet.

Servizzi ta' Sejbien ta' l-Intrużjonijiet

Il-CSIRTs li jwettqu dan is-servizz jeżaminaw IDS logs eżistenti, janalizzaw u jibdew rispons għal kwalunkwe episodju li jilħaq il-limitu definit tagħhom, jew jibagħtu allarmi skond ftehim definit minn qabel dwar il-livell ta' servizz jew strateġija ta' eskalazzjoni. Is-sejbien ta' l-intrużjonijiet u l-analiżi tar-rekords relatati tas-sigurtà tista' tkun biċċa xogħol li taqta' qalb dak li jkun – mhux biss fl-istabbiliment ta' fejn issib is-sensuri fl-ambjent, iżda wkoll fil-ġbir u mbagħad l-analiżi ta' l-ammonti kbar ta' informazzjoni maqbuda. F'ħafna każijiet, huma meħtieġa għodod u għarfien speċjalizzat biex tiġi sintetizzata u interpretata l-informazzjoni sabiex jiġu identifikati allarmi foloz, attakki, jew episodji fin-netwerk u biex jiġu implimentati strateġiji sabiex jitneħħew jew jitnaqqsu dawn l-avvenimenti. Xi organizzazzjonijiet jagħżlu li jikkuntrattaw din l-attività lil partijiet oħra li jkollhom aktar kompetenza fit-twettiq ta' dawn is-servizzi, bħal fornituri ta' servizzi tas-sigurtà ġestiti.

Tixrid ta' Informazzjoni Relatata mas-Sigurtà

Dan is-servizz jipprovdi lill-kostitwenti b'ġabra komprensiva u faċli biex issibha ta' informazzjoni utli li tgħin biex tittejjeb is-sigurtà. Informazzjoni bħal din tista' tinkludi

- rappurtar ta' linji gwida u informazzjoni ta' kuntatt għall-CSIRT
- arkivji ta' allarmi, twissijiet, u dikjarazzjonijiet oħra
- dokumentazzjoni dwar l-aħjar prattiċi kurrenti
- gwida ġenerali dwar is-sigurtà tal-kompjuters
- politiki, proċeduri, u listi ta' kontroll
- żvilupp ta' soluzzjonijiet u informazzjoni dwar it-tqassim
- links tal-bejjiegħ
- statistiċi u xejriet kurrenti fir-rappurtar ta' l-inċidenti
- tagħrif ieħor li jista' jtejjeb il-prattiċi ġenerali tas-sigurtà

Din l-informazzjoni tista' tiġi żviluppata u ppubblikata mill-CSIRT jew minn parti oħra ta' l-organizzazzjoni (IT, riżorsi umani, jew relazzjonijiet mal-medja), u tista' tinkludi informazzjoni minn sorsi esterni bħal CSIRTs oħra, bejjiegħa, u esperti tas-sigurtà.

Servizzi ta' Ġestjoni tal-Kwalità tas-Sigurtà

Is-servizzi li jaqgħu f'din il-kategorija mhumiex esklussivi għall-immaniġġar ta' l-inċidenti jew għall-CSIRTs b'mod partikolari. Huma servizzi stabbiliti magħrufin sewwa, imfassla sabiex itejbu s-sigurtà ġenerali ta' organizzazzjoni. Billi juża l-esperjenzi miksuba fl-għoti tas-servizzi reattivi u s-servizzi proattivi deskritti fuq, CSIRT jista' jforni perspettivi uniċi għal dawn is-servizzi ta' ġestjoni tal-kwalità li altrimenti ma kinux ikunu disponibbli. Dawn is-servizzi huma mfasslin biex jinkorporaw il-kummenti u l-lezzjonijiet meħuda fuq il-bażi ta' l-għarfien miksub bir-rispons għall-inċidenti, il-vulnerabilitajiet u l-attakki. L-inseriment ta' esperjenzi bħal dawn fis-servizzi tradizzjonali stabbiliti (ara taħt) bħala parti minn proċess għall-ġestjoni tal-kwalità tas-sigurtà jista' jtejjeb l-isforzi tas-sigurtà fuq perjodu fit-tul ta' organizzazzjoni. Jiddependi fuq l-istrutturi u r-responsabbiltajiet organizzattivi, CSIRT jista' jipprovdi dawn is-servizzi jew jipparteċipa bħala parti minn sforz ta' tim organizzattiv akbar.
Id-deskrizzjonijiet li ġejjin jispjegaw kif il-kompetenza tal-CSIRT tista' tkun ta' benefiċċju għal kull wieħed minn dawn is-servizzi ta' ġestjoni tal-kwalità tas-sigurtà.

Analiżi tar-Riskju

Il-CSIRTs jistgħu jkunu kapaċi li jżidu l-valur għall-analiżi u l-evalwazzjonijiet tar-riskju. Dan jista' jtejjeb il-ħila ta' l-organizzazzjoni li tevalwa t-theddidiet reali, li tipprovdi stimi kwalitattivi u kwantitattivi realistiċi tar-riskji għall-assi ta' l-informazzjoni, u li tevalwa l-istrateġiji tal-protezzjoni u r-rispons. Il-CSIRTs li jwettqu dan is-servizz jagħmlu jew jassistu f'attivitajiet ta' analiżi tar-riskju għas-sigurtà ta' l-informazzjonji għal sistemi ġodda u proċessi tan-negozju jew jevalwaw it-theddidiet u l-attakki kontra l-assi u s-sistemi tal-kostitwenti.

Ippjanar għall-Kontinwità tan-Negozju u l-Irkupru minn Diżastru

Fuq il-bażi ta' okkorrenzi mgħoddija u previżjonijiet futuri tax-xejriet emerġenti dwar l-inċidenti jew is-sigurtà, aktar u aktar inċidenti għandhom il-potenzjal li jirriżultaw f'degradazzjoni serja ta' l-operazzjonijiet tan-negozju. Għalhekk, l-isforzi ta' l-ippjanar għandhom iqisu l-esperjenza u r-rakkomandazzjonijiet tal-CSIRT meta jistabbilixxu l-aħjar mod kif wieħed jirrispondi għal tali inċidenti biex tkun żgurata l-kontinwità fl-operazzjonijiet tan-negozju. Il-CSIRTs li jwettqu dan is-servizz huma involuti fl-ippjanar għall-kontinwità tan-negozju u l-irkupru minn diżastru għal avvenimenti relatati mat-theddidiet u l-attakki għas-sigurtà tal-kompjuters.

Konsulenzi dwar is-Sigurtà

Il-CSIRTs jistgħu jintużaw sabiex jipprovdu parir u gwida dwar l-aħjar prattiċi li għandhom jiġu implimentati għall-operazzjonijiet tan-negozju tal-kostitwenti. CSIRT li jagħti dan is-servizz huwa involut fit-tħejjija ta' rakkomandazzjonijiet jew l-identifikazzjoni tar-rekwiżiti sabiex jinxtraw, jiġu installati, jew protetti sistemi ġodda, apparat tan-netwerk, applikazzjonijiet tas-softwer, jew proċessi tan-negozju għall-intrapriża kollha. Dan is-servizz jinkludi l-għoti ta' gwida u assistenza fl-iżvilupp tal-politiki dwar is-sigurtà ta' l-organizzazzjoni jew il-kostitwenza. Jista' jinvolvi wkoll l-għoti ta' xhieda jew pariri lil korpi leġislattivi jew governattivi oħra.

Tkabbir ta' l-Għarfien

Il-CSIRTs jistgħu jkunu kapaċi jidentifikaw fejn il-kostitwenti jeħtieġu aktar gwida u informazzjoni sabiex jikkonformaw aħjar ma' prattiċi aċċettati dwar is-sigurtà u mal-politika ta' l-organizzazzjoni dwar is-sigurtà. It-tkabbir ta' l-għarfien ġenerali dwar is-sigurtà tal-popolazzjoni kostitwenti mhux biss iżid il-ftehim tagħhom dwar kwistjonijiet ta' sigurtà iżda jgħinhom ukoll sabiex iwettqu l-operazzjonijiet tagħhom ta' kuljum b'mod aktar sigur. Dan jista' jnaqqas is-seħħ ta' attakki li jirnexxu u jżid il-probabbiltà li l-kostitwenti jiskopru u jirrapportaw l-attakki, biex hekk inaqqsu l-ħinijiet ta' l-irkupru u jeliminaw jew inaqqsu t-telf.
Il-CSIRTs li jwettqu dan is-servizz ifittxu opportunitajiet sabiex iżidu l-għarfien dwar is-sigurtà billi jiżviluppaw artikli, kartelluni, bullettini ta' informazzjoni, websajts, jew riżorsi informattivi oħra li jispjegaw l-aħjar prattiċi tas-sigurtà u jipprovdu parir dwar il-prekawzjonijiet li għandhom jittieħdu. L-attivitajiet jistgħu jinkludu wkoll skedar ta' attivitajiet u seminars sabiex il-kostitwenti jinżammu aġġornati mal-proċeduri li hemm fir-rigward tas-sigurtà u t-theddidiet potenzjali għas-sistemi organizzattivi.

Edukazzjoni/Taħriġ

Dan is-servizz jinvolvi l-għoti ta' informazzjoni lill-kostitwenti dwar kwistjonijiet ta' sigurtà tal-kompjuters permezz ta' seminars, *workshops*, korsijiet, u *tutorials*. Is-suġġetti jistgħu jinkludu linji gwida għar-rappurtar ta' l-inċidenti, metodi xierqa ta' rispons, għodod ta' rispons għall-inċidenti, metodi ta' prevenzjoni ta' l-inċidenti, u tagħrif ieħor neċessarju biex wieħed jipproteġi, jiskopri, jirrapporta, u jirrispondi għall-inċidenti ta' sigurtà tal-kompjuters.

Evalwazzjoni jew Ċertifikazzjoni tal-Prodott

Għal dan is-servizz, il-CSIRT jista' jagħmel evalwazzjonijiet tal-prodott fuq għodod, applikazzjonijiet, jew servizzi oħra sabiex jiżgura s-sigurtà tal-prodotti u l-konformità tagħhom ma' prattiċi ta' sigurtà aċċettati tal-CSIRT jew organizzattivi. L-għodod u l-applikazzjonijiet evalwati jistgħu jkunu open source jew prodotti kummerċjali. Dan is-servizz jista' jiġi pprovdut bħala evalwazzjoni jew permezz ta' programm ta' ċertifikazzjoni, jiddependi fuq l-istandards li jkunu applikati mill-organizzazzjoni jew mill-CSIRT.

A.3 L-eżempji

CSIRT Fittizju

Pass 0 – Fehim ta' x'inhu CSIRT:

Il-CSIRT kampjun irid jaqdi istituzzjoni medja magħmula minn persunal ta' 200 ruħ. L-istituzzjoni għandha d-dipartiment ta' l-IT tagħha stess u żewġ uffiċċji fergħat oħra fl-istess pajjiż. L-IT għandu rwol fundamentali għall-kumpanija minħabba li jintuża għall-komunikazzjoni interna, netwerk ta' l-informazzjoni u e-negozju 24x7. L-istituzzjoni għandha n-netwerk tagħha stess u tiddisponi minn kollegament żejjed ma' l-internet permezz ta' żewp ISPs differenti.

- -

Pass 1: Fażi tal-bidu

Fil-fażi inizjali l-CSIRT il-ġdid ikun ippjanat bħala CSIRT intern, li jipprovdi s-servizzi tiegħu lill-kumpanija li tospitah, lid-dipartiment lokali ta' l-IT u lill-persunal. Huwa jsostni u jikkoordina wkoll l-immaniġġar ta' inċidenti relatati mas-sigurtà ta' l-IT bejn l-uffiċċji tal-fergħat differenti.

- -

Pass 2: Għażla tas-servizzi korretti

Fil-fażi tal-bidu ġie deċiż li l-CSIRT il-ġdid jiffoka prinċipalment fuq li jipprovdi xi wħud mis-servizzi bażiċi għall-impjegati.

Ġie deċiż li wara fażi pilota tista' tiġi kkunsidrata l-estensjoni tal-portafoll ta' servizzi u jistgħu jiżdiedu Servizzi ta' Ġestjoni tas-Sigurtà. Dik id-deċiżjoni ssir fuq il-bażi tal-kummenti mill-kostitwenti-pilota u f'kollaborazzjoni mill-qrib mad-dipartiment għall-Assigurazzjoni tal-Kwalità.

- -

Pass 3: Issir analiżi tal-kostitwenza u tal-kanali xierqa ta' komunikazzjoni

Sessjoni ta' *brainstorming* ma' wħud mill-persuni prinċipali ta' l-amministrazzjoni u l-kostitwenza ġġenerat biżżejjed input għal analiżi SWOT. Din wasslet għall-konklużjoni li hemm ħtieġa għas-servizzi bażiċi:

- Allarmi u twissijiet
- Ġestjoni ta' l-inċident (analiżi, appoġġ tar-rispons u koordinament tar-rispons)
- Dikjarazzjonijiet

Irid jiġi assigurat li l-informazzjoni tiġi distribwita b'mod organizzat biex tilħaq l-akbar parti possibbli tal-kostitwenza. Għalhekk ittieħdet id-deċiżjoni li allarmi, twissijiet u dikjarazzjonijiet fil-forma ta' konsulenzi dwar is-sigurtà jiġu ppubblikati fuq websajt iddedikata u mqassma permezz ta' lista ta' l-impustar. Il-CSIRT jiffaċilita l-email, it-telefon u l-faks biex jirċievi r-rapporti ta' l-inċidenti. Hija ppjanata formola tal-web integrata għall-pass li jmiss.

Pass 4: Dikjarazzjoni tal-Missjoni

It-tmexxija tal-CSIRT fittizju għamlet id-dikjarazzjoni tal-missjoni segwenti:
"CSIRT Fittizju jipprovdi tagħrif u assistenza lill-persunal tal-kumpanija li tospitah biex inaqqas ir-riskji ta' inċidenti tas-sigurtà fil-kompjuters kif ukoll jirrispondi għal tali inċidenti meta jseħħu."

B'din, il-CSIRT fittizju jagħmilha ċara li huwa CSIRT intern u li x-xogħol prinċipali tiegħu huwa li jieħu ħsieb kwistjonijiet relatati mas-sigurtà ta' l-IT.

- -

Pass 5: Definizzjoni tal-Pjan Korporattiv

Il-mudell finanzjarju
Minħabba l-fatt li l-kumpanija għandha e-kummerċ 24x7 kif ukoll dipartiment ta' l-IT 24x7, ġie deċiż li jkun ipprovdut servizz sħiħ waqt il-ħinijiet tax-xogħol u servizz *on-call* għal wara l-ħinijiet tax-xogħol. Is-servizzi għall-kostitwenza se jkunu pprovduti bla ħlas, iżda l-possibilità li jingħataw servizzi lil klijenti esterni se tiġi evalwata matul il-fażi pilota u ta' l-evalwazzjoni.

Il-mudell tad-dħul
Matul il-fażi tal-bidu u l-fażi pilota l-CSIRT se jkun iffinanzjat permezz tal-kumpanija li tospitah. Matul il-fażi pilota u ta' l-evalwazzjoni se jiġi diskuss finanzjament addizzjonali, fosthom il-possibilità li jinbiegħu servizzi lil klijenti esterni.

Il-mudell organizzattiv
L-organizzazzjoni ospitanti hija kumpanija żgħira, għalhekk intgħażel il-mudell integrat. Waqt il-ħinijiet tax-xogħol, staff ta' tliet persuni ser jipprovdi s-servizzi bażiċi (għoti ta' pariri dwar is-sigurtà u immaniġġar/koordinament ta' l-inċidenti).

Id-dipartiment ta' l-IT tal-kumpanija diġà jħaddem persuni b'ħiliet adegwati. Sar ftehim ma' dak id-dipartiment sabiex il-CSIRT il-ġdid ikun jista' jitlob appoġġ fuq bażi *ad-hoc* meta jkun meħtieġ. Tista' tintuża wkoll it-tieni linja tat-teknixins *on call* tagħhom.
Se jkun hemm tim CSIRT bażiku b'erba' membri *full-time* u ħames membri addizzjonali tat-tim CSIRT. Wieħed minnhom se jkun disponibbli wkoll fuq xift li jdur.

Il-persunal
Il-mexxej tal-CSIRT għandu sfond fis-sigurtà u appoġġ ta' l-ewwel u t-tieni livell u għamel xogħol fil-qasam ta' l-immaniġġar ta' kriżijiet ta' reżistenza. It-tliet membri l-oħra tat-tim huma speċjalisti tas-sigurtà. Min-naħa tagħhom, il-membri tat-tim *part-time* tal-CSIRT mid-dipartiment ta' l-IT huma speċjalisti ta' l-infrastruttura tal-kumpanija.

Pass 5 Użu tal-politika dwar l-uffiċċju u s-sigurtà ta' l-informazzjoni
It-tagħmir ta' l-uffiċċju u l-post
Minħabba li l-kumpanija ospitanti diġà għandha sigurtà fiżika effiċjenti fis-seħħ, il-CSIRT il-ġdid huwa kopert sewwa f'dak ir-rigward. Hekk imsejħa "kamra tal-gwerra" hija pprovduta sabiex tippermetti koordinazzjoni f'każ ta' emerġenza. Inxtara sejf għall-materjal tal-kodifikazzjoni u dokumenti sensittivi. Ġiet stabbilita linja tat-telefon separata li tinkludi swiċċbord biex jiffaċilita l-*hotline* waqt il-ħinijiet tax-xogħol u t-telefon mobbli "*on-call*" għall-ħin barra mill-ħinijiet tax-xogħol bl-istess numru tat-telefon.

Jista' jintuża wkoll tagħmir eżistenti u l-websajt korporattiva sabiex tixxandar informazzjoni relatata mal-CSIRT. Ġiet installata u miżmuma lista ta' l-impustar, b'parti ristretta għall-komunikazzjoni bejn il-membri tat-tim u ma' timijiet oħra. Id-dettalji ta' kuntatt kollha tal-membri tal-persunal huma maħżuna f'database; b'kopja stampata tinżamm fis-sejf.

Regolament
Minħabba li l-CSIRT huwa inkorporat f'kumpanija li diġà għandha politiki dwar is-sigurtà ta' l-informazzjoni, il-politiki relattivi għall-CSIRT ġew stabbiliti bl-għajnuna tal-konsulent legali tal-kumpanija.
- -
Pass 7 Tiftix għal kooperazzjoni
Bl-użu ta' l-Inventarju ta' ENISA, xi CSIRTs fl-istess pajjiż malajr setgħu jinstabu u jiġu kkuntattjati. Ġiet irranġata żjara fuq il-post ma' wieħed minnhom għall-mexxej tat-tim li ġie mqabbad. Huwa tgħallem dwar l-attivitajiet tal-CSIRT nazzjonali u attenda laqgħa. Din il-laqgħa kienet aktar minn utli biex jiġbor eżempji ta' metodi ta' ħidma u jikseb appoġġ minn għadd ta' timijiet oħra.
- -
Pass 8 Promozzjoni tal-Pjan Korporattiv

Ġie deċiż li jinġabru fatti u figuri mill-istorja tal-kumpanija. Dan huwa aktar minn utli għal ħarsa ġenerali statistika tas-sitwazzjoni tas-sigurtà ta' l-IT. Dan il-ġbir għandu jissokta meta l-CSIRT ikun beda jiffunzjona, sabiex l-istatistika tinżamm aġġornata.

Ġew ikkuntattjati u intervistati CSIRTs nazzjonali oħra dwar il-każijiet tan-negozju tagħhom. Huma pprovdew appoġġ billi kkompilaw xi slajds b'informazzjoni dwar żviluppi riċenti fl-inċidenti tas-sigurtà ta' l-IT u dwar l-ispejjeż ta' l-inċidenti.

F'dan il-każ ta' eżempju ta' CSIRT fittizju ma kienx hemm ħtieġa kbira li t-tmexxija tiġi konvinta dwar l-importanza tan-negozju ta' l-IT, u għalhekk ma kienx diffiċli sabiex tinkiseb l-awtorizzazzjoni għall-ewwel pass. Ġew imħejjija każ korporattiv u pjan tal-proġett, fosthom stima ta' l-ispejjeż tat-twaqqif u l-prezz ta' l-operazzjoni.
- -

Pass 9 Stabbiliment tal-flussi tal-proċess u proċeduri tekniċi u operattivi
CSIRT fittizju jiffoka fuq l-għoti tas-servizzi bażiċi ta' CSIRT:

- Allarmi u Twissijiet
- Dikjarazzjonijiet
- Ġestjoni ta' l-Inċident

It-tim żviluppa proċeduri li jaħdmu sewwa u li jinftiehmu mingħajr tbatija minn kull membru tat-tim. CSIRT fittizju qabbad ukoll espert legali biex jieħu ħsieb ir-responsabbiltajiet u l-politika dwar is-sigurtà ta' l-informazzjoni. It-tim adotta xi għodod utli u sab informazzjoni siewja dwar kwistjonijiet operattivi billi ddiskuta ma' CSIRTs oħra.

Saret *template* fissa għall-konsulenzi dwar is-sigurtà u r-rapporti dwar l-inċidenti. It-tim juża l-RTIR għall-ġestjoni ta' l-inċidenti.

- -

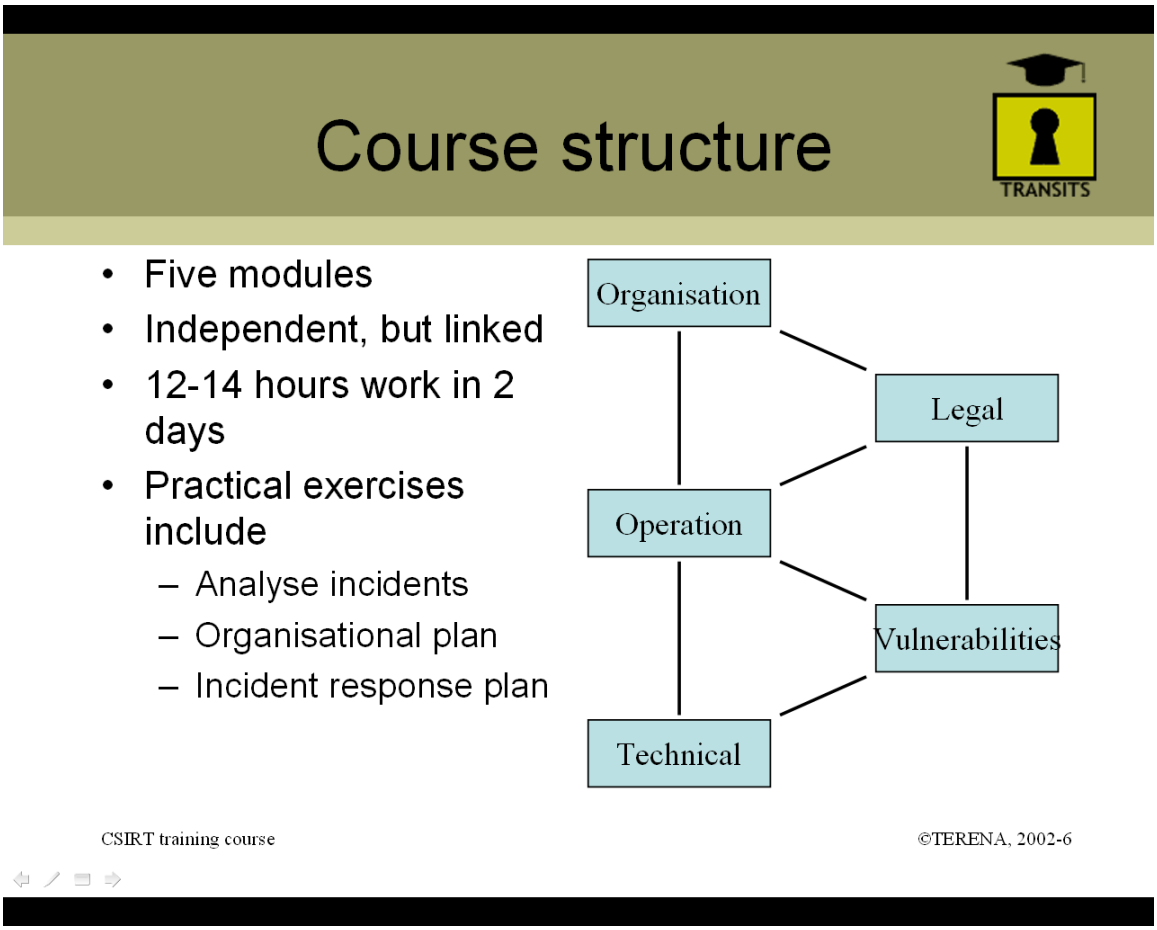
Pass 10 Taħriġ tal-persunal
CSIRT fittizju ddeċieda li jibgħat il-persunal tekniku kollu tiegħu għall-korsijiet ta' TRANSITS. Barra minn hekk il-mexxej tat-tim jattendi l-kors *Kif tmexxi CSIRT* mill-CERT/CC.

- -

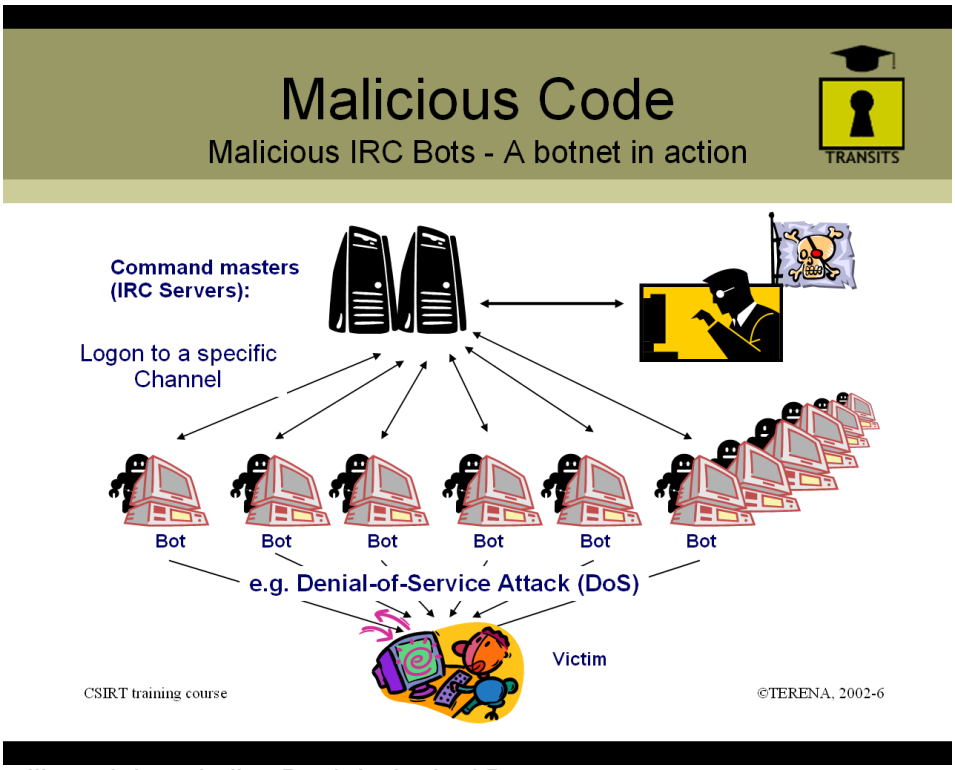
Pass 11: Eżerċizzju
Matul l-ewwel ġimgħat ta' l-operazzjonijiet, il-CSIRT fittizju uża diversi każijiet fittizji (li huma kisbu bħala eżempji minn CSIRTs oħra) li ntużaw bħala eżerċizzju. Barra minn hekk huma ħarġu għadd ta' konsulenzi dwar is-sigurtà bbażati fuq tagħrif reali dwar il-vulnerabilità mqassam minn bejjiegħa tal-ħardwer, li huma adattaw u aġġustaw għall-ħtiġijiet tal-kostitwenza.

A.4 Materjal Kampjun minn Korsijiet tal-CSIRT

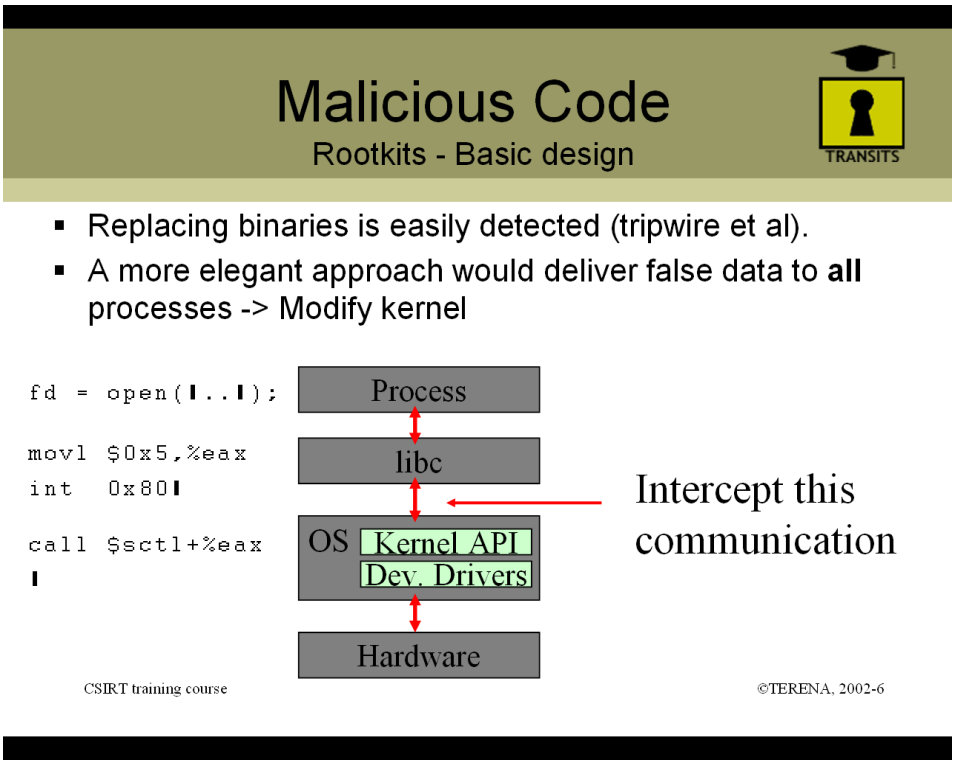
TRANSITS (Bil-permess ġentili ta' Terena, http://www.terena.nl)



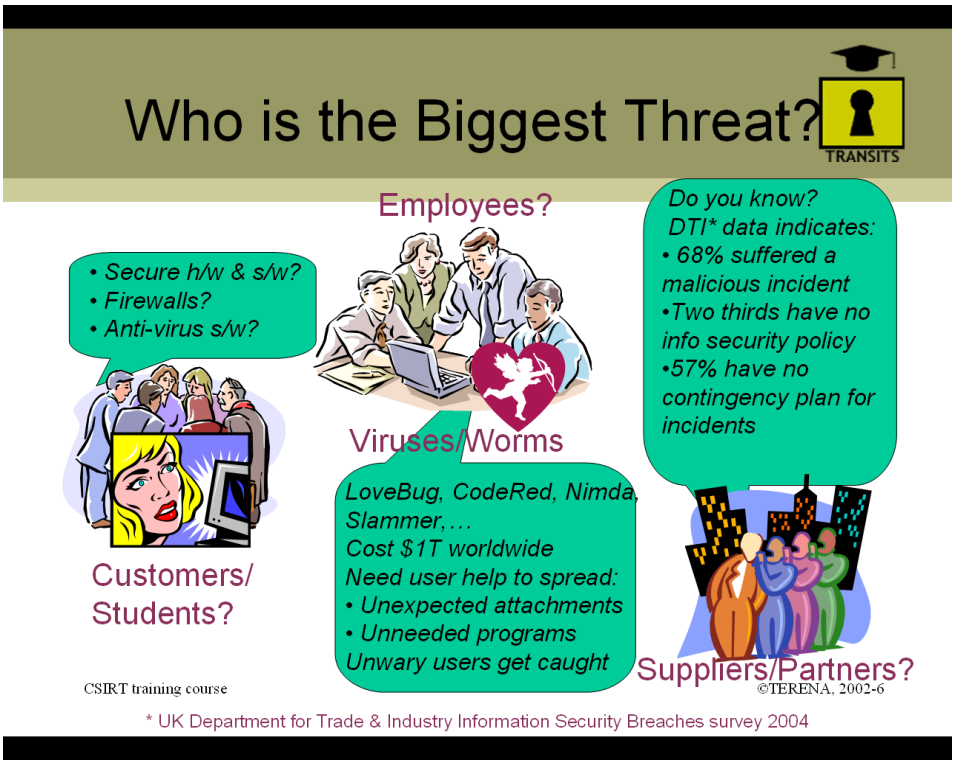
Ħarsa ġenerali: L-istruttura tal-kors



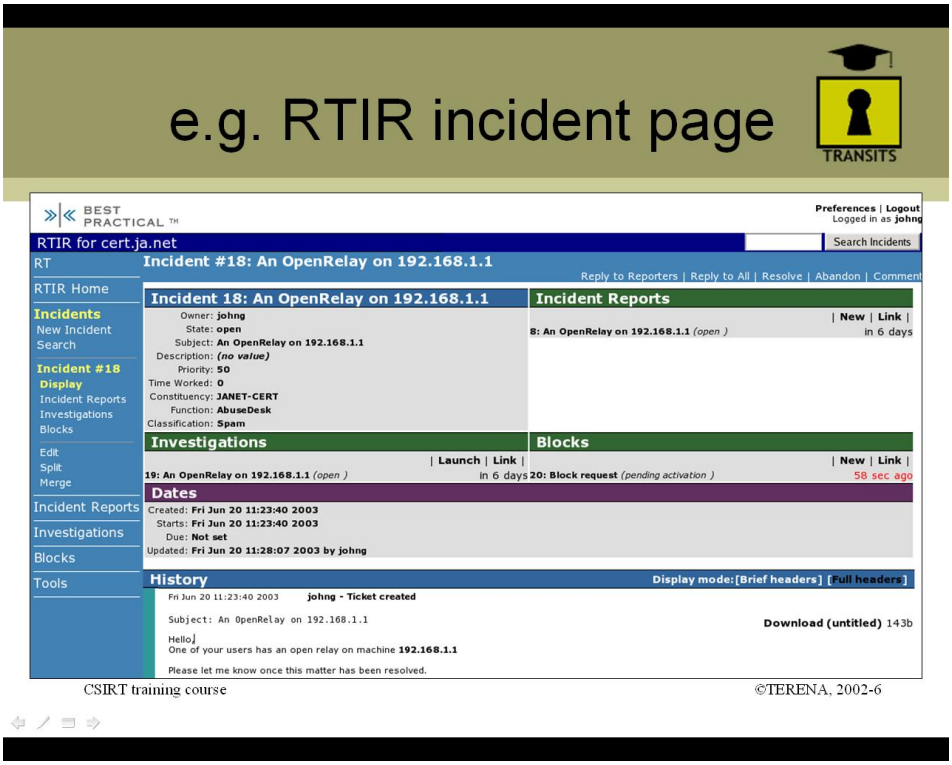
Mill-*Modulu Tekniku*: Deskrizzjoni ta' Botnet



Mill-*Modulu tekniku*: Disinn bażiku ta' *rootkit*



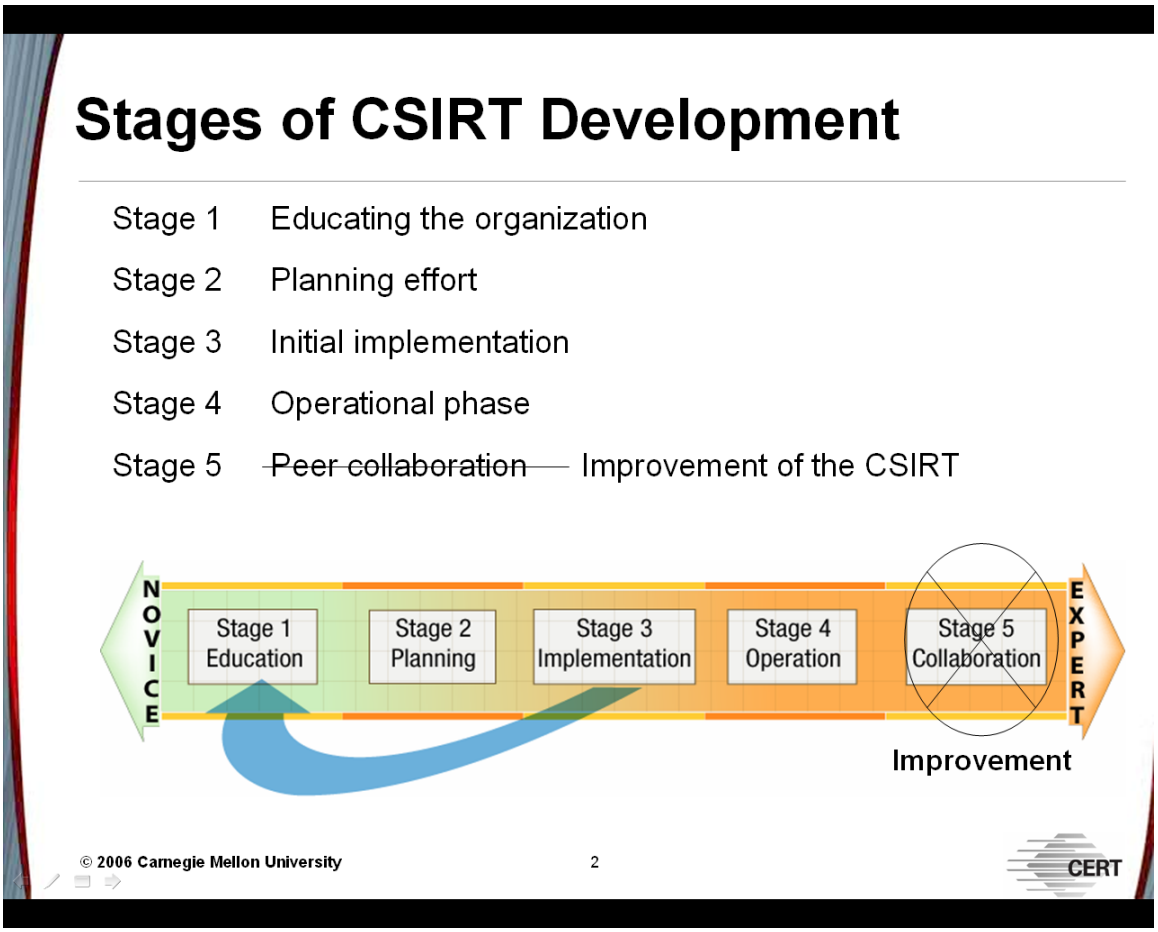
Mill-*Modulu organizzattiv*: Minn ġewwa jew minn barra – fejn qiegħda l-akbar theddida?



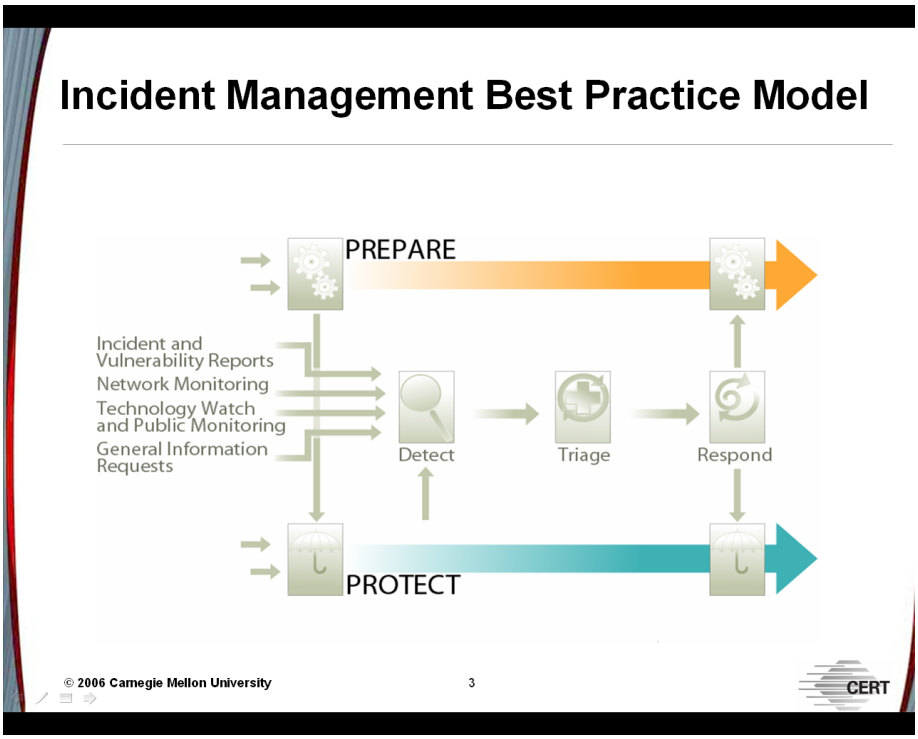
Mit-*Track operattiv*: Request Tracker for Incident Response (RTIR)

"It-twaqqif ta' CSIRTs" (bil-permess ġentili mingħand CERT/CC, http://www.cert.org)

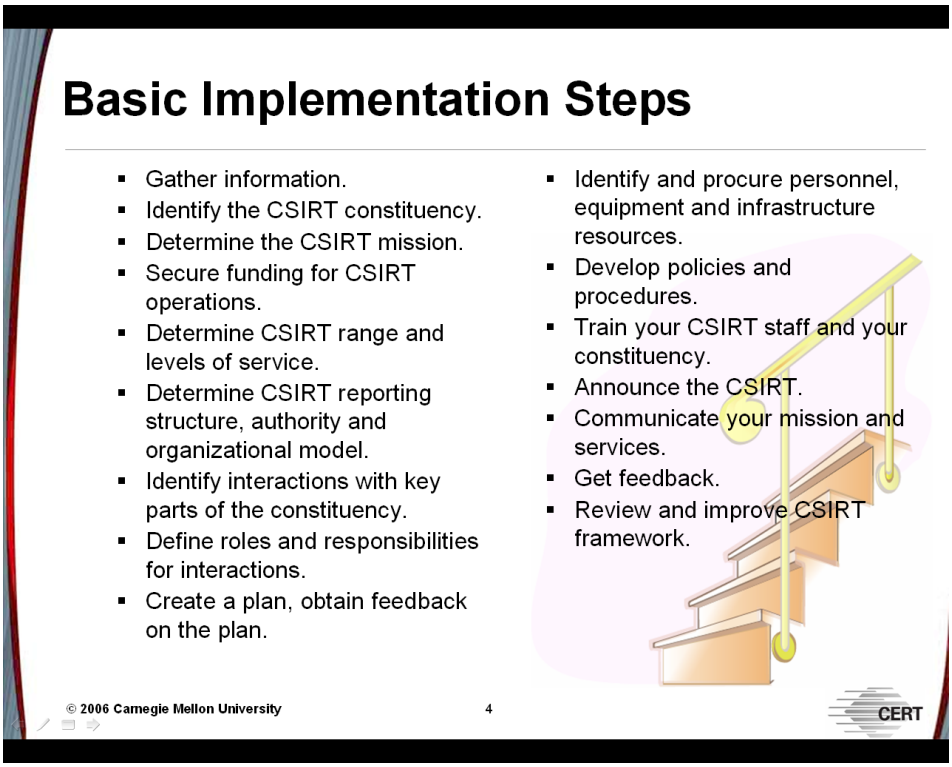
ENISA tirrikonoxxi bi gratitudni lit-Tim ta' Żvilupp tal-CSIRT fil-Programm tal-CERT talli ppermettewlna l-użu ta' kontenut mill-korsijiet ta' taħriġ tagħhom!



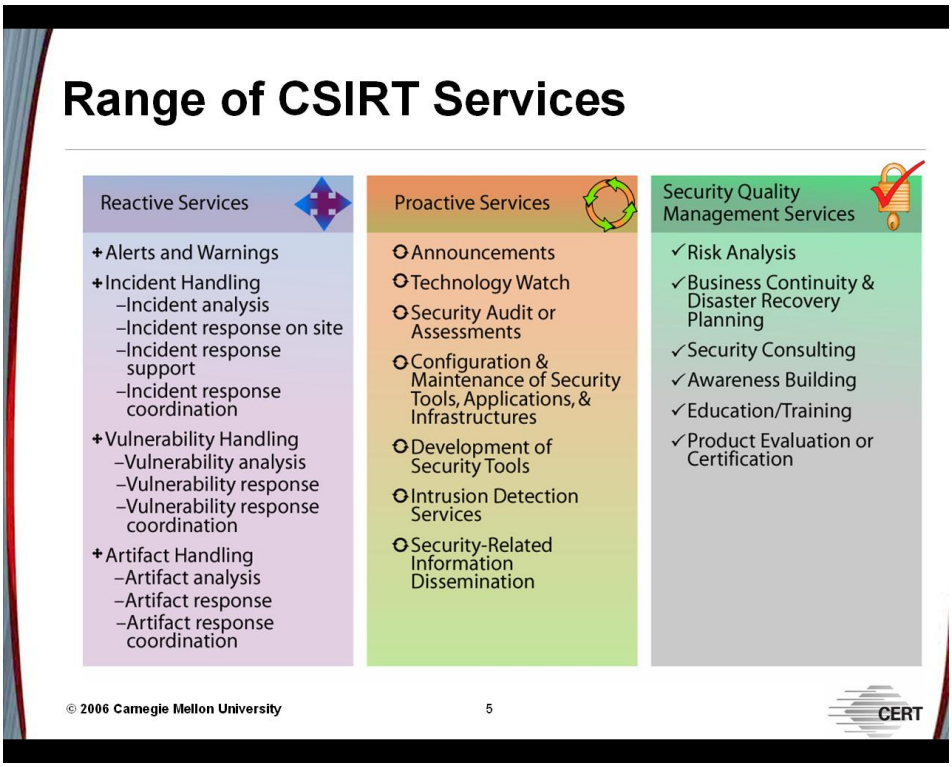
Mill-*Kors ta' Taħriġ* tal-*CERT/CC*: Stadji ta' l-iżvilupp ta' CSIRT



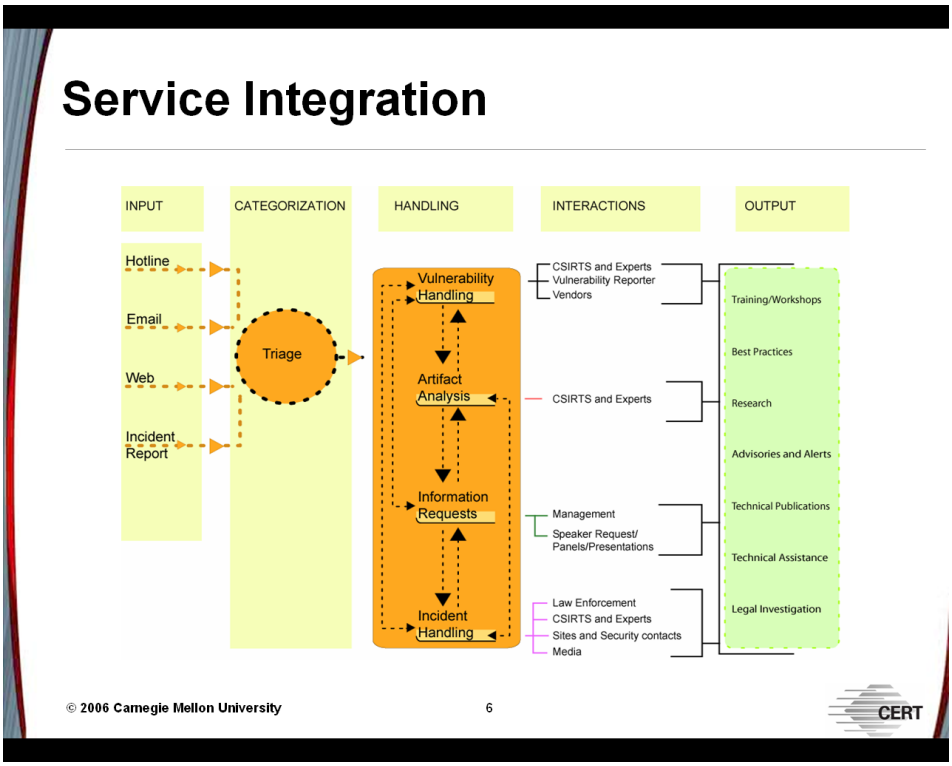
Mill-*Kors ta' Taħriġ* tal-*CERT/CC*: L-aħjar prattika fl-immaniġġar ta' l-inċidenti



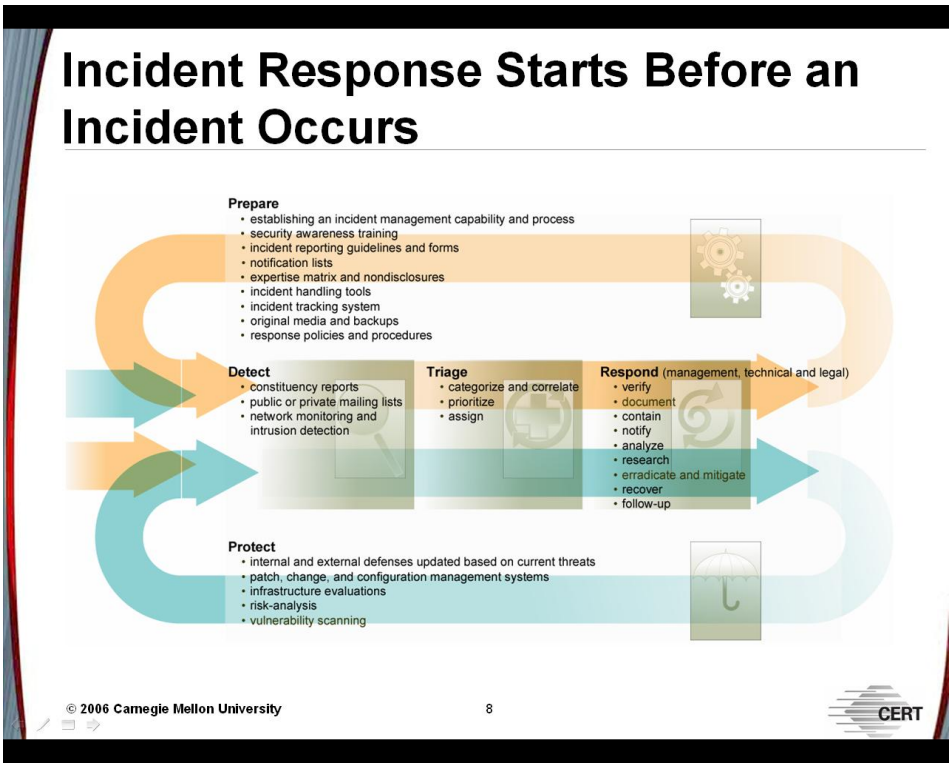
Mill-*Kors ta' taħriġ* tal-*CERT/CC*: Passi li għandhom jiġu segwiti fit-twaqqif ta' CSIRT



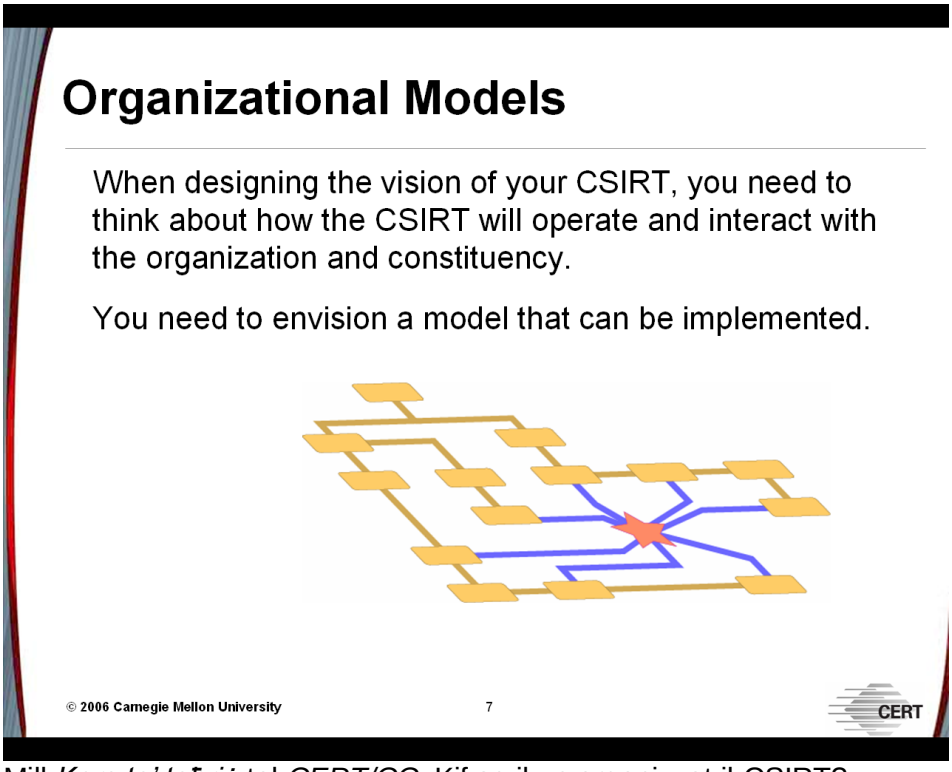
Mill-*Kors ta' taħriġ* tal-*CERT/CC:* Is-servizzi li jista' jipprovdi CSIRT



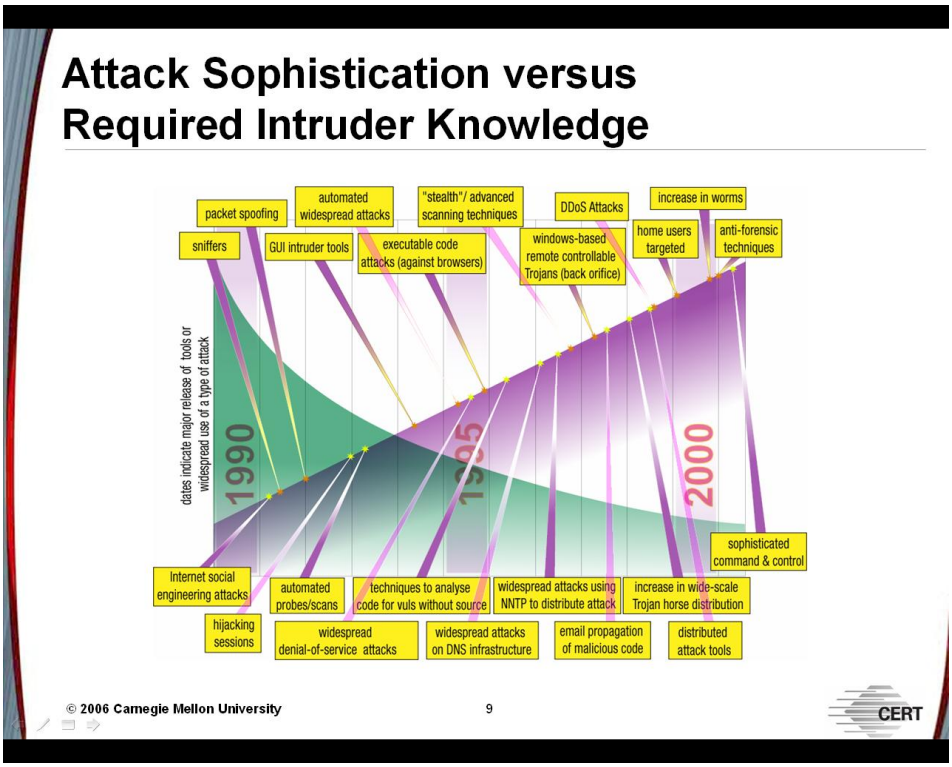
Mill-*Kors ta' taħriġ* tal-*CERT/CC:* Il-fluss tax-xogħol fil-ġestjoni ta' inċident



Mill-*Kors ta' taħriġ* tal-*CERT/CC:* Rispons għall-inċident



Mill-*Kors ta' taħriġ* tal-*CERT/CC:* Kif se jkun organizzat il-CSIRT?



Mill-*Kors ta' taħriġ* tal-*CERT/CC:* Anqas għarfien, aktar ħsara