POSTOPEN PRISTOP K VZPOSTAVITVI CSIRT

Dokument WP2006/5.1(CERT-D1/D2)

Kazalo

1 Povzetek 2

2 Pravna pojasnila 2

3 Zahvala 2

4 Uvod 3

4.1 Ciljna publika 4
4.2 Kako uporabljati ta dokument? 4
4.3 Kako je sestavljen ta dokument 5

5 Splošna strategija pri načrtovanju in vzpostavitvi skupine CSIRT 6

5.1 Kaj je skupina CSIRT? 6
5.2 Morebitne storitve, ki jih lahko zagotavlja CSIRT 10
5.3 Analiza odjemalcev in poslanstvo 12

6 Priprava poslovnega načrta 18

6.1 Priprava finančnega modela 18
6.2 Določitev organizacijske strukture 20
6.3 Zaposlovanje ustreznega osebja 24
6.4 Uporaba pisarne in pisarniška oprema 26
6.5 Razvoj informacijske varnostne politike 28
6.6 Iskanje sodelovanja z drugimi skupinami CSIRT in morebitnimi državnimi pobudami 29

7 Spodbujanje poslovnega načrta 31

7.1 Opis poslovnega načrta in ukrepanje s strani vodstva 33

8 Primeri operativnih in tehničnih postopkov (potek dela) 36

8.1 Dostop do infrastrukture odjemalcev 37
8.2 Priprava alarmov, opozoril in najav 38
8.3 Reševanje incidentov 45
8.4 Primer časovnega razporeda reševanja 51
8.5 Razpoložljivo orodje skupine CSIRT 52

9 Usposabljanje skupine CSIRT 54

9.1 TRANSITS 54
9.2 CERT/CC 55

10 Vaja: priprava svetovanja 56

11 Zaključek 61

12 Opis projektnega načrta 62

PRILOGA 64

A.1 Dodatno branje 64
A.2 Storitve skupine CSIRT 65
A.3 Primeri 74
A.4 Vzorčno gradivo s tečajev skupine CSIRT 78

1 Povzetek

Ta dokument opisuje proces vzpostavitve Skupine za razreševanje varnostnih incidentov (CSIRT) iz različnih vidikov, kot je vidik poslovanja podjetja, upravljanja postopkov in tehnični vidik. Ta dokument izvaja dva dokumenta, opisana v poglavju 5.1 Delovnega načrta agencije ENISA za leto 2006:

- Ta dokument: *Pisno poročilo o postopnem pristopu k vzpostavitvi CERT ali podobnih skupin, vključno s primeri.* (**CERT-D1**)
- Poglavje 12 in zunanje datoteke: *Povzetek načrta, naveden po postavkah, kar omogoča enostavno uporabo načrta v praksi.* (**CERT-D2**)

2 Pravna pojasnila

3 Zahvala

ENISA se zahvaljuje vsem ustanovam in osebam, ki so sodelovale pri pripravi tega dokumenta. Posebna zahvala gre naslednjim avtorjem:

- Henku Bronku, ki je kot svetovalec pripravil prvo različico tega dokumenta.
- CERT/CC, predvsem pa razvojni skupini CSIRT, ki je prispevala večino uporabnega gradiva in vzorčno gradivo za izobraževanje v prilogi.
- GovCERT.NL za posredovanje *CERT-in-a-box*.
- Skupini TRANSITS, ki je v prilogi prispevala vzorce izobraževalnega gradiva.
- Sodelavcem iz skupine za varnostne politike v tehničnem oddelku, ki so pripravili poglavje 6.6.
- Številnim ljudem, ki so pregledali in popravili ta dokument.

4 Uvod

Komunikacijska omrežja in informacijski sistemi so postali bistveni dejavniki pri gospodarskem in socialnem razvoju. Računalniška in omrežna tehnologija sta postali enako razširjeni kot oskrba z elektriko in vodo.

Zaradi tega varnost komunikacijskih omrežij in informacijskih sistemov, predvsem pa njihova razpoložljivost, postaja vse bolj pomembna za družbo. To izhaja iz nevarnosti za nastanek težav na ključnih informacijskih sistemih zaradi celovitosti sistemov, nesreč, napak in napadov na fizične infrastrukture, ki zagotavljajo storitve, ki so ključnega pomena za dobro počutje državljanov EU.

10. marca 2004 je bila ustanovljena Evropska agencija za varnost omrežij in informacij (ENISA)[1]. Zagotavljala naj bi visoko in učinkovito stopnjo informacijske in omrežne varnost znotraj skupnosti in razvila kulturo informacijske in omrežne varnosti, ki bi koristila državljanom, potrošnikom, podjetjem in organizacijam javnega sektorja znotraj Evropske unije, in s tem prispevala k brezhibnemu delovanju notranjega trga.

Številne varnostne skupnosti v Evropi, kot so CERT/CSIRT, skupine za zlorabe in skupine WARP, že več let sodelujejo in si prizadevajo za varnejši internet. ENISA bo te skupnosti pri njihovih prizadevanjih podpirala tako, da jim bo posredovala informacije o ukrepih za zagotavljanje ustrezne ravni kakovosti storitev. Poleg tega namerava ENISA povečati svojo sposobnost za svetovanje državam članicam EU in zadevnim organom EU pri zagotavljanju ustreznih varnostnih storitev posebnim skupinam uporabnikov informacijske tehnologije. Zaradi tega bo ta nova delovna skupina gradila na ugotovitvah začasne delovne skupine za sodelovanje in podporo CERT, ustanovljene leta 2005, in tako obravnavala vprašanja, ki se nanašajo na zagotavljanje ustreznih varnostnih storitev („storitev CERT“) posebnim (kategorijam ali skupinam) uporabnikom.

Z objavo tega svojega poročila „*Postopna vzpostavitev skupine CSIRT z dodatnim kontrolnim seznamom*“, ENISA podpira ustanavljanje novih skupin CSIRT, z njegovo pomočjo pa boste lahko vzpostavili lastno skupino CSIRT.

[1] Uredba (ES) št. 460/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij. „Agencija Evropske skupnosti“ je organ, ki ga je ustanovila EU, da bi opravljal posebne tehnične, znanstvene ali vodstvene naloge na "področju Skupnosti" ("prvi steber") EU.

4.1 Ciljna publika

Glavne ciljne skupine tega poročila so vladne in druge ustanove, ki se odločajo o vzpostavitvi skupine CSIRT, da bi na ta način zaščitile svojo informacijsko-tehnološko infrastrukturo ali infrastrukturo svojih partnerjev.

4.2 Kako uporabljati ta dokument?

Ta dokument vsebuje informacije o tem, kaj je skupina CSIRT, katere storitve lahko zagotavlja in kateri koraki so potrebni za začetek njenega delovanja. To daje bralcu dober in pragmatičen pregled nad pristopom, strukturo in vsebino o tem, kako vzpostaviti CSIRT.

Poglavje 4 „*Uvod*“
Uvod v to poročilo

Poglavje 5 „*Splošna strategija pri načrtovanju in vzpostavitvi skupine CSIRT“*
Prvi del opisuje, kaj je skupina CSIRT. Prav tako vsebuje informacije o različnih okoljih, v katerih lahko deluje skupina CSIRT, in storitvah, ki jih lahko zagotavlja.

Poglavje 6 „*Razvoj poslovnega načrta“*
To poglavje opisuje pristop vodstva podjetja pri vzpostavitvi.

Poglavje 7 „*Spodbujanje poslovnega načrta“*
To poglavje obravnava poslovni primer in vprašanja financiranja.

Poglavje 8 „*Primeri operativnih in tehničnih postopkov*“
To poglavje opisuje postopek pridobivanja informacij in njihovo preoblikovanje v varnostna sporočila. Prav tako opisuje potek dela pri razreševanju incidentov.

Poglavje 9 „*Usposabljanje skupine CSIRT*“
To poglavje vsebuje povzetek razpoložljivega usposabljanja CSIRT. Za ilustracijo je v prilogi podan primer izobraževalnega gradiva.

Poglavje 10 „*Vaja: priprava nasveta*“
To poglavje vsebuje vajo na temo, kako izvesti eno izmed osnovnih (ali temeljnih) storitev skupine CSIRT: priprava varnostnega sporočila (ali nasveta).

Poglavje 12 *„Opis poslovnega načrta“*
To poglavje opisuje dodatni projektni načrt (kontrolni seznam), ki je priložen tem navodilom. Namen tega načrta je zagotoviti enostavno orodje, ki ga je mogoče uporabljati pri izvajanju teh navodil.

4.3 Kako je sestavljen ta dokument

Vsako poglavje se začne s povzetkom korakov, ki so bili v postopku vzpostavitve skupine CSIRT že izvedeni, kar je bralcem v veliko pomoč. Ti povzetki so izpisani v okvirih na naslednji način:

Opravili smo prvi korak.

Vsako poglavje se konča s praktičnim primerom že obravnavanih korakov. V tem dokumentu kot „navidezno skupino CSIRT“ uporabljamo majhno, neodvisno skupino CSIRT za srednje veliko podjetje ali ustanovo. Povzetek lahko najdete v prilogi.

Navidezna skupina CSIRT

5 Splošna strategija pri načrtovanju in vzpostavitvi skupine CSIRT

Za uspešen začetek postopka vzpostavitve skupine CSIRT je pomembno imeti jasno vizijo možnih storitev, ki jih lahko skupina zagotavlja svojim strankam, ki so v „svetu CSIRT“ bolj znane pod imenom „odjemalci“. Zaradi tega je treba za pravočasno zagotavljanje ustreznih storitev, ki so primerne kakovosti, razumeti potrebe odjemalcev.

5.1 Kaj je skupina CSIRT?

CSIRT je kratica za Skupino za reševanje varnostnih incidentov. Kratica CSIRT se v Evropi uporablja predvsem za zaščiten izraz CERT, ki ga je v ZDA registriral Koordinacijski center CERT (CERT/CC).
Obstajajo različne okrajšave, ki se uporabljajo za isto vrsto skupin:

- CERT ali CERT/CC (Center za posredovanje pri internetnih incidentih / koordinacijski center).
- CSIRT (Skupina za reševanje varnostnih incidentov)
- IRT (Skupina za reševanje incidentov)
- CIRT (Skupina za reševanje računalniških incidentov)
- SERT (Skupina za reševanje varnostnih vprašanj)

Do prvega večjega izbruha črva v globalni informacijsko-tehnološki infrastrukturi je prišlo konec osemdesetih let prejšnjega stoletja. Črv je bil poimenovan Morris[2] in se je hitro širil, pri tem pa okužil veliko število sistemov IT po vsem svetu.

Ta incident je deloval kot budnica: ljudje so se nenadoma zavedli močne potrebe po sodelovanju in usklajevanju med sistemskimi administratorji in vodji IT z namenom reševanja takšnih primerov. Ker je bil čas ključni dejavnik, je bilo treba vzpostaviti bolj organiziran in strukturiran pristop k reševanju varnostnih incidentov IT. Tako je nekaj dni po „incidentu Morris“ Agencija za napredne obrambne analize (DARPA) vzpostavila prvo CSIRT: Koordinacijski center CERT (CERT/CC[3]) s sedežem na Univerzi Carnegie Mellon v Pittsburghu (Pensilvanija).

Ta model je bil hitro prevzet po Evropi in v letu 1992 je nizozemski akademski ponudnik SURFnet vzpostavil prvi CSIRT v Evropi, poimenovan SURFnet-CERT[4]. Temu je sledilo veliko skupin in trenutno *Seznam dejavnosti CERT v Evropi*[5] vsebuje več kot 100 poznanih skupin znotraj Evrope.

Z leti so CERT razširile svoje zmogljivosti od izključno reakcijskih skupin do popolnega ponudnika varnostnih storitev, vključno s preventivnimi storitvami, kot so opozorila, varnostno svetovanje, usposabljanje in storitve upravljanja varnosti. Izraz „CERT“ je kmalu postal nezadosten. Kot rezultat je bil ob koncu devetdesetih let prejšnjega stoletja

[2] Več informacij o črvu Morris lahko najdete na http://en.wikipedia.org/wiki/Morris_worm

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

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

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

uveden nov pojem „CSIRT“. Sedaj se oba izraza (CERT in CSIRT) uporabljata kot sopomenki, pri čemer pa je CSIRT bolj natančen izraz.

5.1.1 Pojem *odjemanja*

Od sedaj se bo (v skupnostih CSIRT) za bazo strank skupine CSIRT uporabljal dobro uveljavljen izraz „odjemalci“. Ena sama stranka bo naslovljena kot „odjemalec“, skupina kot „odjemalci“.

5.1.2 Opredelitev CSIRT

CSIRT je skupina varnostnih strokovnjakov IT, katerih glavna naloga je odzivanje na računalniške varnostne incidente. Zagotavlja potrebne storitve za njihovo reševanje in nudi podporo svojim odjemalcem pri odpravi kršitev.

Z namenom omejevanja tveganj in čim večjega zmanjšanja števila potrebnih odzivov večina skupin CSIRT svojim odjemalcem zagotavlja tudi preventivne in izobraževalne storitve. Pripravljajo nasvete glede ranljivosti programske in strojne opreme, ki je v uporabi, prav tako pa obveščajo uporabnike o zlorabah in virusih, ki izkoriščajo te pomanjkljivosti. Tako lahko odjemalci hitro popravijo in posodobijo svoje sisteme. Za popoln seznam možnih storitev si oglejte poglavje *5.2 Možne storitve*.

5.1.3 Prednosti vzpostavitve CSIRT

Delovanje IT varnostne ekipe pomaga organizaciji pri omejevanju in preprečevanju večjih incidentov in pri varovanju dragocenih sredstev.

Druge morebitne prednosti so:

- Centralizirano usklajevanje varnostnih vprašanj IT znotraj organizacije (kontaktno mesto, PoC).
- Centralizirano in specializirano obravnavanje in odzivanje na incidente IT.
- Dostopno strokovno znanje, ki omogoča podporo in nudenje pomoči uporabnikom za hitro odpravo varnostnih incidentov.
- Obravnava pravnih vprašanj in ohranjanje dokazov v primeru tožb.
- Spremljanje razvoja na področju varnosti.
- Spodbujanje sodelovanja med odjemalci na področju varnosti IT (dviganje osveščenosti).

Navidezna CSIRT (0. korak)
Razumevanje, kaj je skupina CSIRT: Vzorčna CSIRT bo služila potrebam srednje velike ustanove, ki jo sestavlja 200 članov osebja. Ustanova ima svoj oddelek IT in še dve drugi poslovalnici v isti državi. IT v podjetju igra ključno vlogo, saj se uporablja za notranjo komunikacijo, podatkovno omrežje in e-poslovanje 24 ur na dan, 7 dni v tednu. Ustanova ima svoje omrežje in razpolaga z redundančno povezavo do interneta prek dveh različnih ponudnikov internetnih storitev.

5.1.4 Opis različnih vrst okolij, v katerih deluje CSIRT

Opravili smo prvi korak.

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.

>> Naslednji korak je podati odgovor na vprašanje: „Kateremu sektorju bo skupina CSIRT zagotavljala storitve?“

Ob vzpostavitvi skupine CSIRT (prav tako kot pri vsakem drugem podjetju) je zelo pomembno, da se zelo hitro izoblikuje stališče o tem, kdo so odjemalci in za kakšno okolje se bodo razvijale storitve skupine CSIRT. Trenutno razlikujemo med naslednjimi navedenimi „sektorji“:

- CSIRT za akademski sektor
- Komercialna skupina CSIRT
- CSIRT za sektor CIP/CIIP
- CSIRT za vladni sektor
- Notranja skupina CSIRT
- CSIRT za vojaški sektor
- Nacionalna skupina CSIRT
- CSIRT za sektor malih in srednje velikih podjetij (MSP)
- CSIRT za trgovski sektor

CSIRT za akademski sektor
Poudarek
CSIRT za akademski sektor zagotavlja storitve skupine CSIRT akademskim in izobraževalnim ustanovam, kot so univerze ali raziskovalne ustanove, ter njihovim internetnim okoljem.

Odjemalci
Običajni odjemalci za to vrsto skupine CSIRT so študentje in osebje na univerzah.

Komercialna skupina CSIRT
Poudarek
Komercialna skupina CSIRT svojim odjemalcem zagotavlja komercialne storitve skupine CSIRT. V primeru ponudnika internetnih storitev CSIRT v glavnem zagotavlja storitve za preprečevanje zlorabe končnim uporabnikom (klicna povezava, ADSL) in storitve skupine CSIRT svojim profesionalnim strankam.

Odjemalci
Komercialne skupine CSIRT običajno zagotavljajo svoje storitve odjemalcem, ki zanje plačajo.

CSIRT za sektor CIP/CIIP
Poudarek
Skupine CSIRT v tem sektorju so predvsem osredotočene na varovanje ključnih informacij in/ali varovanje ključnih informacij in infrastrukture. Ta specializirana skupina CSIRT v večini primerov tesno sodeluje z vladnim oddelkom CIIP. Pokriva vse ključne sektorje IT v državi in ščiti državljane te države.

Odjemalci
Vlada, ključna informacijsko-tehnološka podjetja, državljani

CSIRT za vladni sektor
Poudarek
Vladna skupina CSIRT zagotavlja storitve vladnim agencijam, v nekaterih državah pa tudi državljanom.

Odjemalci
Vlada in vladne agencije; v nekaterih državah so storitve opozarjanja zagotovljene tudi državljanom (na primer v Belgiji, na Madžarskem, na Nizozemskem, v Združenem kraljestvu ali v Nemčiji).

Notranja skupina CSIRT
Poudarek
Notranja skupina CSIRT zagotavlja storitve samo svoji organizaciji gostiteljici. To bolj opisuje delovanje kot pa sektor. Veliko telekomunikacijskih organizacij in bank ima svoje notranje skupine CSIRT. Običajno te skupine nimajo spletne strani, ki bi bila dostopna javnosti.

Odjemalci
Notranje osebje in informacijsko-tehnološki oddelek organizacije gostiteljice.

CSIRT za vojaški sektor
Poudarek
CSIRT v tem sektorju zagotavlja storitve vojaškim organizacijam z odgovornostmi za infrastrukturo IT, ki se uporablja v obrambne namene.

Odjemalci
Osebje vojaških ustanov ali tesno povezani subjekti, kot je na primer oddelek za obrambo.

Nacionalna skupina CSIRT
Poudarek
Skupina CSIRT z nacionalnim poudarkom šteje kot varnostno kontaktno mesto za državo. V nekaterih primerih tudi vladna skupina CSIRT deluje kot nacionalno kontaktno mesto (kot UNIRAS v Združenem kraljestvu).

Odjemalci
Ta vrsta skupine CSIRT običajno nima neposrednih odjemalcev, saj nacionalna skupina CSIRT igra le posredniško vlogo za celotno državo.

CSIRT za sektor malih in srednje velikih podjetij (MSP)
Poudarek
Samoorganizirana skupina CSIRT, ki zagotavlja storitve podružnici svojega podjetja ali podobni uporabniški skupini.

Odjemalci
Odjemalci teh skupin CSIRT so lahko MSP in njihovo osebje ali posebne interesne skupine, kot je „skupnost mest in občin“ države.

CSIRT za trgovski sektor
Poudarek
CSIRT za trgovski sektor je osredotočena na podporo izdelkom, značilnih za posamezne trgovce. Cilj je običajno razviti in zagotoviti storitve z namenom odpravljanja ranljivosti in omejevanja morebitnih negativnih vplivov zaradi pomanjkljivosti.

Odjemalci
Lastniki izdelkov

Kot je opisano v odstavku o nacionalnih skupinah CSIRT, lahko skupina deluje tudi v različnih sektorjih. To na primer vpliva na analize odjemalcev in njihovih potreb.

Navidezna CSIRT (1. korak)
Začetna faza V začetni fazi se nova skupina CSIRT načrtuje kot notranja skupina CSIRT, ki zagotavlja svoje storitve družbi gostiteljici, lokalnemu oddelku IT in osebju. Prav tako nudi podporo in usklajuje reševanje varnostnih incidentov, povezanih z IT, med različnimi podružnicami.

5.2 Morebitne storitve, ki jih lahko zagotavlja CSIRT

Opravili smo prva dva koraka.

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.
2. Kateremu sektorju bo skupina CSIRT zagotavljala storitve?

>> Naslednji korak je podati odgovor na vprašanje, *kakšne storitve zagotavljati odjemalcem*.

Obstajajo številne storitve, ki jih lahko zagotavlja CSIRT, vendar trenutno še nobena obstoječa skupina CSIRT ne zagotavlja vseh. Zaradi tega je izbira ustreznega nabora storitev ključnega pomena. Spodaj boste našli kratek pregled znanih storitev, ki jih zagotavljajo skupine CSIRT, kot so opredeljene v „priročniku za skupine CSIRT“, ki ga je objavil CERT/CC[6].

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

Reaktivne storitve	**Proaktivne storitve**	**Ravnanje s komponentami**
• **Alarmi in opozorila** • **Reševanje incidentov** • **Analiza incidentov** • **Podpora pri odzivanju na incidente** • **Usklajevanje odziva na incidente** • Reševanje incidenta na mestu samem • Odpravljanje ranljivosti • Analiziranje ranljivosti • Odzivanje na ranljivosti • Usklajevanje odziva na ranljivosti	• **Najave** • Spremljanje tehnologije • Varnostni pregledi ali ocene • Konfiguracija in vzdrževanje varnosti • Razvoj varnostnih orodij • Storitve odkrivanja vdorov • Razširjanje informacij povezanih z varnostjo	• *Analize komponent* • *Odziv na komponente* • *Usklajevanje odziva na komponente* ***Obvladovanje varnosti in kakovosti*** • *Analiza tveganj* • *Zagotavljanje neprekinjenega delovanja in ponovna vzpostavitev po nesreči* • *Varnostno svetovanje* • *Dvigovanje osveščenosti* • *Izobraževanje/usposabljanje* • *Ocenjevanje ali certificiranje produkta*

Slika 1 Seznam storitev CSIRT povzet po CERT/CC[7]

Osnovne storitve (označene s krepko pisavo): Razlikujemo med reaktivnimi in proaktivnimi storitvami. Proaktivne storitve so namenjene preprečevanju incidentov z dvigovanjem osveščenosti in usposabljanjem, medtem ko so reaktivne storitve namenjene reševanju incidentov in omejevanju nastale škode.

Ravnanje s komponentami obsega analizo vseh datotek ali objektov, ki so v sistemu in ki bi lahko bili del zlonamernih dejanj, kot so ostanki virusov, črvov, ukaznih datotek, trojancev itd. Prav tako obsega distribucijo in ravnanje s pridobljenimi informacijami prodajalcev in drugih vpletenih strank z namenom preprečevanja nadaljnjega širjenja škodljive programske opreme in zmanjševanja tveganj.

Storitve obvladovanja varnosti in kakovosti so storitve z dolgoročnejšimi cilji in obsegajo svetovalne in izobraževalne ukrepe.

Za podrobnosti o razlagi storitev CSIRT glejte prilogo.

Izbira pravih storitev za vaše odjemalce je pomemben korak in bo nadalje obravnavan v poglavju *6.1 Določitev finančnega modela*.

Večina skupin CSIRT začne s posredovanjem „alarmov in opozoril“, „objavljanjem“ in „reševanjem incidentov“ pri svojih odjemalcih. Te ključne storitve običajno zagotavljajo dober profil in stopnjo pozornosti pri odjemalcih ter v glavnem štejejo kot prava „dodana vrednost“.

Vzpostavitev majhne skupine „poskusnih“ odjemalcev, posredovanje ključnih storitev za poskusno časovno obdobje in pridobivanje povratnih informacij velja za dobro prakso.

[7] Sezam storitev CSIRT povzet po CERT/CC: http://www.cert.org/csirts/services.html

Zainteresirani poskusni uporabniki običajno posredujejo tvorne povratne informacije in pomagajo pri razvoju odjemalcem prilagojene storitve.

Navidezna CSIRT (2 korak)
Izbira pravih storitev V začetni fazi je sprejeta odločitev, da bo CSIRT osredotočena predvsem na zagotavljanje nekaterih osnovnih storitev zaposlenim. Po poskusni fazi se sprejme odločitev o razširitvi nabora storitev, doda pa se lahko tudi storitev „obvladovanja varnosti“. Ta odločitev bo sprejeta na osnovi povratnih informacij poskusnih odjemalcev in v tesnem sodelovanju z oddelkom za zagotavljanje kakovosti.

5.3 Analiza odjemalcev in poslanstvo

Opravili smo prve tri korake:

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.
2. Kateremu sektorju bo skupina CSIRT zagotavljala storitve?
3. Katere storitve lahko CSIRT zagotavlja svojim odjemalcem.

>> Naslednji korak je podati odgovor na vprašanje, *kakšen pristop izbrati pri vzpostavitvi CSIRT*?

Naslednji korak je podrobnejši pregled odjemalcev z glavnim ciljem izbrati ustrezne komunikacijske kanale:

- Opredelitev komunikacijskega pristopa k odjemalcem.
- Določitev poslanstva.
- Priprava realnega izvedbenega/projektnega načrta.
- Določitev storitev skupine CSIRT.
- Določitev organizacijske strukture.
- Opredelitev informacijske varnostne politike.
- Zaposlovanje ustreznega osebja.
- Uporaba pisarne skupine CSIRT.
- Iskanje sodelovanja z drugimi skupinami CSIRT in morebitnimi državnimi pobudami.

Ti koraki bodo podrobneje opisani v naslednjih odstavkih in jih je mogoče uporabljati kot vhodne informacije pri podjetju – in projektnem načrtu.

5.3.1 Komunikacijski pristop k odjemalcem

Kot je bilo že prej navedeno, je zelo pomembno poznati potrebe odjemalcev, prav tako pa tudi svojo lastno komunikacijsko strategijo, vključno s komunikacijskimi kanali, ki so najbolj primerni za posredovanje informacij odjemalcem.

Teorija upravljanja pozna različne možne pristope za reševanje problema analiziranja ciljne skupine. V tem dokumentu bomo opisali dva takšna pristopa: Analizi SWOT in PEST.

Analiza SWOT
Analiza SWOT je orodje za strateško načrtovanje, ki se uporablja za ocenjevanje prednosti (**S**trenghts) in slabosti (**W**eaknesses), priložnosti (**O**pportunities) in nevarnosti (**T**hreats) pri projektu ali poslovni dejavnosti ali v vseh drugih okoliščinah, kjer je potrebna odločitev. Razvoj tehnike se pripisuje Albertu Humphreyju, ki je v šestdesetih in sedemdesetih letih prejšnjega stoletja na univerzi v Stanfordu vodil raziskovalni projekt, pri čemer je uporabljal podatke podjetij na lestvici Fortune 500.[8]

Prednosti	**Slabosti**
Priložnosti	**Nevarnosti**

Slika 2 Analiza SWOT

[8] Definicija analize SWOT na spletni strani Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Analiza PEST

Analiza PEST je drugo pomembno in široko uporabljeno orodje za analiziranje odjemalcev z namenom razumevanja **p**olitičnega, **e**konomskega, **s**ociološko-kulturnega in **t**ehnološkega okolja, v katerem deluje skupina CSIRT. Pomaga pri določevanju, ali je načrtovanje še vedno usklajeno z okoljem, in po možnosti omogoča izogibanje izvajanju akcij na osnovi napačnih predpostavk.

Politično	**Ekonomsko**
• Ekološka/okoljska vprašanja • Trenutna zakonodaja na notranjem trgu • Prihodnja zakonodaja • Evropska/mednarodna zakonodaja • Regulatorni organi in procesi • Vladne politike • Mandat in zamenjava vlade • Trgovinske politike • Financiranje, subvencije in pobude • Interesne/lobirajoče skupine na notranjem trgu • Mednarodne interesne skupine	• Stanje domačega gospodarstva • Smernice domačega gospodarstva • Prekomorska gospodarstva in smernice • Splošna davčna vprašanja • Obdavčitve, ki se nanašajo na posamezne izdelke/storitve • Sezonska/vremenska vprašanja • Tržni in prodajni cikli • Dejavniki za posamezne industrijske panoge • Tržne poti in distribucijske smernice • Zahteve kupcev/končnih uporabnikov • Obrestne mere in tečaji
Sociološko	**Tehnološko**
• Smernice življenjskega sloga • Demografija • Odnosi in mnenja strank • Mnenja medijev • Socialni dejavniki, ki vplivajo na spremembe zakonov • Podoba blagovne znamke, podjetja, tehnologije • Nakupni vzorci strank • Moda in vzorniki • Pomembnejši dogodki in vplivi • Možnost nakupov in smernice • Etnični/verski dejavniki • Oglaševanje in obveščanje javnosti	• Razvoj konkurenčnih tehnologij • Financiranje raziskav • Spremljajoče/odvisne tehnologije • Nadomestne tehnologije/rešitve • Zrelost tehnologije • Zrelost in zmogljivost proizvodnje • Informiranje in komuniciranje • Stranke, ki kupujejo mehanizme/tehnologijo • Zakonodaja, ki se nanaša na tehnologijo • Inovacijski potencial • Dostop, licenciranje, patenti za tehnologije • Vprašanja o intelektualni lastnini

Slika 3 Model analize PEST

Podroben opis analize PEST lahko najdete na spletni strani Wikipedia[9].

Obe orodji podajata celovit in strukturiran pregled nad potrebami odjemalcev. Rezultati bodo dopolnjevali poslovno priložnost in s tem pomagali pri pridobivanju finančnih sredstev pri vzpostavitvi skupine CSIRT.

Komunikacijski kanali

Pomembno temo v teh analizah predstavljajo možne komunikacijske metode in metode distribucije informacij („Kako komunicirati z odjemalci?“)

[9] Definicija analize PEST na spletni strani Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Dobro je izvajati tudi osebne obiske pri odjemalcih, če je to mogoče. Dokazano dejstvo je, da osebna srečanja olajšajo sodelovanje. Če sta obe strani pripravljeni na sodelovanje, lahko ta srečanja vodijo do bolj odprtih medsebojnih odnosov.

Običajno skupine CSIRT uporabljajo večje število komunikacijskih kanalov. Naslednje rešitve so se v praksi izkazale kot uporabne, zato je o njih vredno razmisliti:

- spletno mesto, namenjeno javnosti;
- zaprta območja za člane na spletnem mestu;
- spletni forumi, kjer je mogoče prijaviti incidente;
- seznami poštnih naslovov;
- elektronska pošta po meri;
- telefon / telefaks;
- SMS
- „tradicionalna“ pisma v papirni obliki;
- mesečna ali letna poročila.

Poleg uporabe elektronske pošte, spletnih forumov, telefonov ali telefaksov, ki olajšajo reševanje incidentov (za prejemanje poročil o incidentih s strani odjemalcev, usklajevanje z drugimi skupinami ali posredovanje povratnih informacij in podporo žrtvam), večina skupin CSIRT na poštnih seznamih in javno dostopnih spletnih mestih objavlja tudi svoje varnostne svetovalce.

! Če je le mogoče, se informacije razpošiljajo na varen način. Elektronski pošti je mogoče dodati digitalni podpis s tehnologijo PGP, občutljive podatke o incidentih pa je treba vedno pošiljati šifrirane.

Več informacij je mogoče najti v poglavju *8.5 Orodja, ki so na voljo skupini CSIRT.* Glejte tudi poglavje *2.3* dokumenta *RFC2350*[10].

Navidezna CSIRT (3.a korak)

Izvajanje analiz odjemalcev in ustrezni komunikacijski kanali

Na sestanku viharjenja možganov z nekaj ključnimi vodilnimi osebami in odjemalci je bilo zbranih dovolj vhodnih informacij za izvedbo analiz SWOT. Posledica tega je ugotovitev, da obstaja potreba po ključnih storitvah:

- obveščanje in opozorila,
- reševanje incidentov (analiza, podpora pri pripravi odziva in usklajevanje odzivov),
- najave.

Treba je zagotoviti, da se informacije posredujejo na dobro organiziran način, ki zajema največje možno število odjemalcev. Sprejeta je odločitev, da bodo alarmi, opozorila in najave v obliki nasvetov glede varnosti objavljeni na namenskem spletnem mestu in distribuirani prek poštnega seznama. Za prejemanje poročil o incidentih skupina CSIRT

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

uporablja e-pošto, telefon in telefaks. Kot naslednji korak se načrtuje priprava poenotenega spletnega obrazca.

Na naslednji strani si oglejte analizo SWOT.

Prednosti • Znotraj podjetja obstaja določeno znanje. • Načrt jim je všeč in so pripravljeni sodelovati. • Financiranje in podpora s strani uprave.	**Slabosti** • Med različnimi oddelki in podružnicami ne poteka ustrezna komunikacija. • Brez usklajevanja incidentov IT. • Veliko „majhnih oddelkov“.
Priložnosti • Velik obseg nestrukturiranih občutljivih informacij. • Močna potreba po usklajevanju. • Zmanjševanje izgub zaradi incidentov. • Veliko odprtih vprašanj glede varnosti IT. • Izobraževanje osebja glede varnosti IT.	**Nevarnosti** • Na voljo je premalo denarja. • Premalo osebja. • Velika pričakovanja. • Kultura.

Slika 4 Primer analize SWOT.

5.3.2 Izjava o poslanstvu

Naslednji korak po analiziranju potreb in želja odjemalcev, ki se nanašajo na storitve skupine CSIRT, je priprava osnutka izjave o poslanstvu.

Poslanstvo opisuje osnovno delovanje organizacije znotraj družbe z vidika proizvodov in storitev, ki jih zagotavlja svojim odjemalcem. Omogoča jasno posredovanje informacij o obstoju in delovanju nove skupine CSIRT.

Priprava poslanstva, ki je celovito, pa vendar ne preveč omejujoče, je dobra praksa, saj bo ostalo nespremenjeno več let.

Tu boste našli nekaj primerov poslanstev delujočih skupin CSIRT:

„<Naziv skupine CSIRT> svojim <odjemalcem (določite svoje odjemalce)> nudi informacije in pomoč pri izvajanju proaktivnih ukrepov, namenjenih zmanjševanju tveganj za računalniške varnostne incidente, prav tako pa se odziva na takšne incidente, kadar do njih pride.“

„Zagotavljanje podpore <odjemalcem> na področju preprečevanja in odzivanje na varnostne incidente, ki so povezani z informacijsko tehnologijo.“[11]
Poslanstvo predstavlja zelo pomemben in potreben začetni korak. Podroben opis o tem, katere informacije morajo skupine CSIRT objavljati, lahko najdete v poglavju *2.1* dokumenta *RFC2350*[12] .

Navidezna CSIRT (3.b korak)
Vodstvo navidezne skupine CSIRT je pripravilo naslednjo izjavo o poslanstvu: *„Navidezna skupina CSIRT nudi osebju svojih gostujočih podjetij informacije in pomoč pri zmanjševanju tveganj za računalniške varnostne incidente, prav tako pa se odziva na takšne incidente, kadar do njih pride.“* S tem navidezna skupina CSIRT jasno opredeljuje, da je notranja skupina CSIRT in da je njena glavna dejavnost reševanje vprašanj, povezanih z informacijsko tehnologijo.

[11] Poslanstvo skupine Govcert.nl: http://www.govcert.nl

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

6 Priprava poslovnega načrta

Opravili smo naslednje korake:

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.
2. Kateremu sektorju bo skupina CSIRT zagotavljala storitve?
3. Katere storitve lahko CSIRT zagotavlja svojim odjemalcem.
4. Analiziranje okolja in odjemalcev.
5. Določitev poslanstva.

>> Naslednji korak je priprava poslovnega načrta.

Rezultati analiz vam dajejo dober pregled nad potrebami in (domnevnimi) pomanjkljivostmi odjemalcev, zaradi česar se v naslednjem koraku uporabljajo kot vhodni podatki.

6.1 Priprava finančnega modela

Po opravljenih analizah je bilo za začetek izbranih nekaj osnovnih storitev. Naslednji korak je preučitev finančnega modela: kateri parametri zagotavljanja storitev so primerni in plačljivi.

V popolnem svetu bi bilo financiranje prilagojeno potrebam odjemalcev, v realnosti pa je treba nabor storitev, ki jih je mogoče zagotoviti, prilagoditi zagotovljenemu proračunu. Zaradi tega je bolj stvarno začeti z načrtovanjem finančnih vprašanj.

6.1.1 Stroškovni model

Dva glavna dejavnika, ki vplivata na stroške, sta določitev ur obratovanja in število (ter kakovost) osebja, ki bo zaposleno. Ali obstaja potreba po zagotavljanju odziva 24 ur na dan, 7 dni v tednu na incidente in tehnično podporo ali bodo te storitve na voljo le med uradnimi urami?

Glede na želeno razpoložljivost in opremljenost pisarne (ali je na primer mogoče delati tudi od doma?) lahko uporaba urnika dela na poziv ali rednega urnika dela prinaša določene prednosti.

V času uradnih ur je smiselno zagotavljati tako proaktivne, kot tudi reaktivne storitve. Izven uradnih ur bodo člani osebja zagotavljali le omejene storitve na poziv, na primer samo ob večjih nesrečah in incidentih.

Druga možnost je iskanje mednarodnega sodelovanja z drugimi skupinami CSIRT. Primeri delujočega sodelovanja „Following the Sun“ že obstajajo. Na primer sodelovanje med skupinami v Evropi in Ameriki se je izkazalo za koristno in zagotavlja dober način za izmenjavo obstoječih zmogljivosti. Skupina CSIRT Sun Microsystems, ki ima številne podružnice v različnih časovnih conah po svetu (vse pa so članice iste skupine CSIRT), izvaja storitve 24 ur na dan, 7 dni v tednu z nenehnim izmenjevanjem dolžnosti med

skupinami po vsem svetu. S tem zmanjšujejo stroške, saj skupine delajo samo v času običajnih uradnih ur, hkrati pa zagotavljajo storitve delu sveta, ki „trenutno spi“.

Posebna analiza potrebe po storitvah 24 ur na dan, 7 dni v tednu na strani odjemalcev je dobra praksa. Alarmi in opozorila, ki se posredujejo v nočnih urah, niso smiselni, če jih bodo prejemniki prebrali šele naslednje jutro. Obstaja le majhna razlika med „potrebovati storitev“ in „želeti si storitev“, na število potrebnega osebja in prostorov pa zelo veliko prispevajo ravno delovne ure, s tem pa imajo velik vpliv tudi na stroškovni model.

6.1.2 Model prihodkov

Ko so stroški znani, je naslednji dober korak priprava možnega modela prihodkov: kako je mogoče financirati načrtovane storitve. Sledi nekaj možnih scenarijev, ki jih lahko obravnavate:

Uporaba obstoječih virov
Uporaba virov, ki so že na voljo v drugih delih podjetja, vedno prinaša koristi. Ali je primerno osebje s potrebnim ozadjem in izkušnjami (na primer v obstoječem oddelku IT) že zaposleno? Vodstvo bo verjetno lahko našlo rešitev za premestitev tega osebja v skupino CSIRT v začetni fazi, ali pa bo lahko skupini CSIRT zagotavljalo podporo pri posameznih primerih.

Članarina
Zagotavljanje storitev odjemalcem proti plačilu letne/četrtletne članarine predstavlja drugo možnost. Tudi dodatne storitve, kot so na primer svetovalne storitve ali varnostne presoje, je mogoče plačevati po uporabi na osnovi uporabe.

Dodatna smiselna rešitev: Storitve (notranjega) svetovanja se zagotavljajo brezplačno, storitve, ki se zagotavljajo zunanjim strankam, pa so plačljive. Dodatna možnost je objavljanje svetovalnih in informacijskih oglasnih desk na javnih spletnih mestih, hkrati pa priskrbeti oddelek namenjen „samo članom“, ki vsebuje posebne, podrobnejše ali posebej prilagojene informacije.

V praksi je bilo dokazano, da ima pri zagotavljanju ustreznih finančnih sredstev „naročnina na storitev skupine CSIRT“ predvsem v začetni fazi le omejeno uporabnost. Skupina se sooča na primer s stalnimi splošnimi stroški, prav tako pa je treba opremo plačati že vnaprej. S prodajo storitev skupine CSIRT je težko kriti te stroške, prav tako pa je v tem primeru potrebna zelo podrobna finančna analiza, s katero se ugotovi „točka, ko so stroški pokriti".

Subvencije
Druga možnost, o kateri je vredno razmisliti, je prošnja za pridobitev subvencije za projekte, ki jih zagotavlja vlada ali vladni organ, saj danes večina držav namenja sredstva za financiranje projektov za varnost IT. V takem primeru se je dobro obrniti na Ministrstvo za notranje zadeve.

Seveda je možna tudi kombinacija različnih modelov prihodkov.

6.2 Določitev organizacijske strukture

Za skupino CSIRT primerna organizacijska struktura je močno odvisna od obstoječe strukture organizacije gostiteljice in odjemalcev. Prav tako je odvisna od razpoložljivosti usposobljenih strokovnjakov, ki jih je mogoče trajno zaposliti ali najeti za posamezne projekte.

Običajno skupina CSIRT znotraj ekipe opredeli naslednje vloge:

Generalno vodstvo
- Generalni direktor

Osebje
- Vodja pisarne
- Računovodja
- Svetovalec na področju komunikacij
- Pravni svetovalec

Operativna tehnična skupina
- Vodja tehnične skupine
- Tehniki tehnične skupine CSIRT, ki zagotavljajo storitve skupine CSIRT
- Raziskovalci

Zunanji svetovalci
- Zaposleni po potrebi

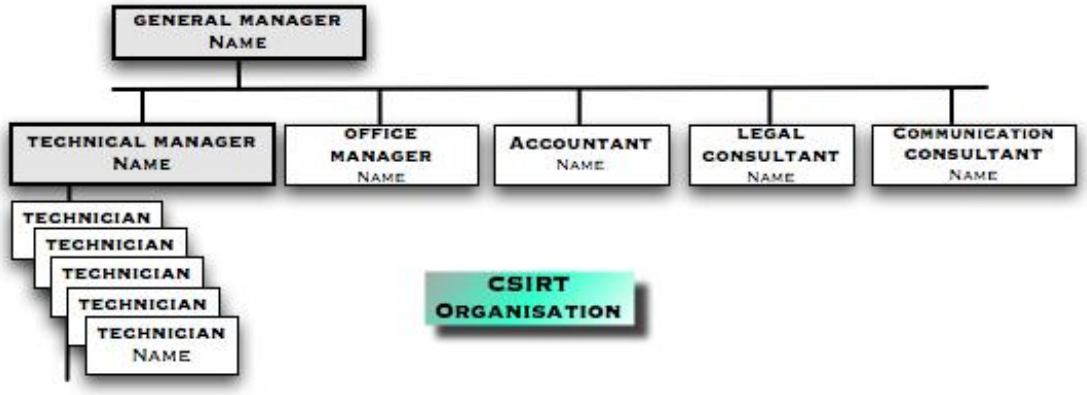
Prisotnost pravnega strokovnjaka v skupini, predvsem v fazi vzpostavitve skupine CSIRT, je zelo pomembna. Zaradi tega bodo stroški sicer višji, vseeno pa bo skupini prihranjen čas in pravne težave.

Prav tako se je v skupini pokazala kot zelo uporabna prisotnost strokovnjaka za komunikacije in sicer glede na različne stopnje usposobljenosti med odjemalci, pa tudi v primeru, ko je skupina CSIRT medijsko izpostavljena. Ti strokovnjaki se lahko osredotočijo na preoblikovanje težjih tehničnih vprašanj v za odjemalce in medijske partnerje lažje razumljiva sporočila. Strokovnjak za komunikacijo bo tehničnim strokovnjakom prav tako nudil povratne informacije s strani odjemalcev, in lahko deluje tudi kot „prevajalec“ ali „posrednik“ med tema dvema skupinama.

Sledi nekaj primerov organizacijskih modelov, ki jih uporabljajo delujoče skupine CSIRT.

6.2.1 Neodvisen poslovni model

Skupina CSIRT je vzpostavljena in deluje kot neodvisna organizacija s svojim vodstvom in zaposlenimi.

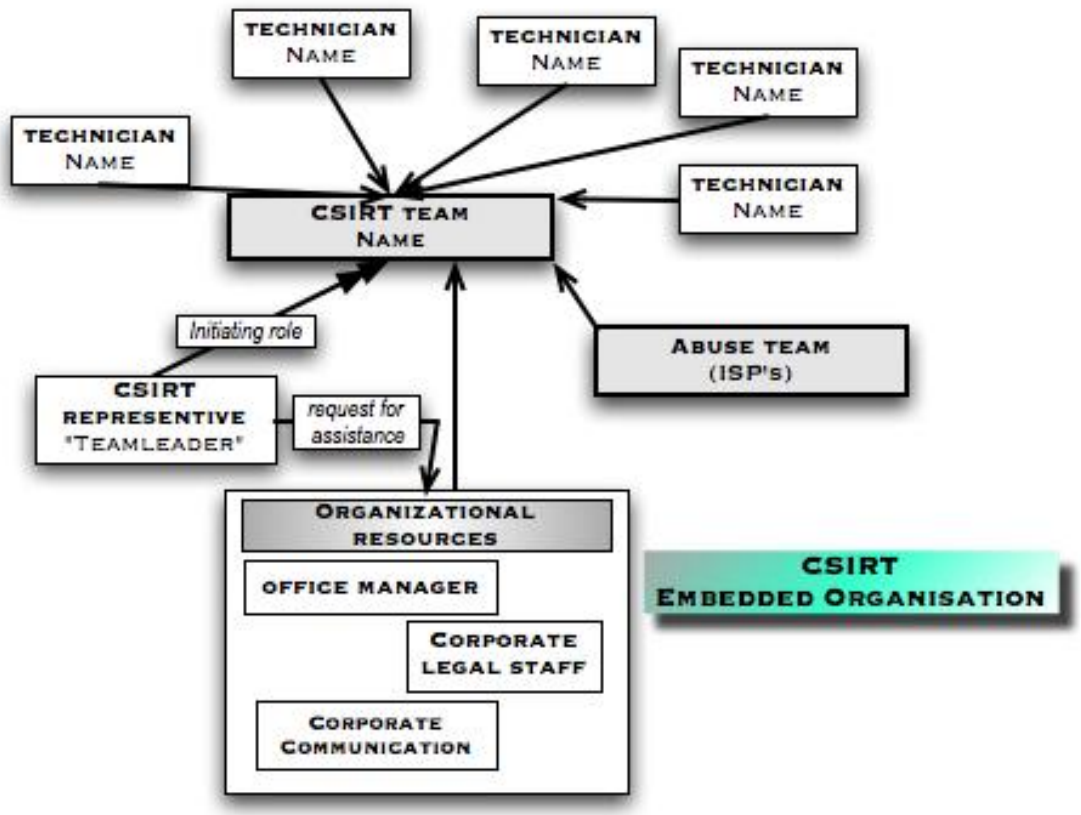


Slika 5 Neodvisni poslovni model

6.2.2 Model vgraditve

Skupina CSIRT lahko uporablja ta model, če bo vzpostavljena znotraj obstoječe organizacije in pri tem na primer uporabljala obstoječ oddelek IT. Na čelu skupine CSIRT je vodja skupine, ki je odgovoren za dejavnosti CSIRT. Vodja skupine je pri reševanju incidentov ali pri pripravi dejavnosti skupine CSIRT zadolžen za pridobivanje potrebnih tehnikov. Za pomoč pri strokovni podpori pa lahko zaprosi znotraj obstoječe organizacije.

Ta model je mogoče uporabljati tudi v posebnih okoliščinah. V tem primeru ima skupina stalno število članov ali ustreznik polnega delovnega časa (FTE). Delo v centru za pomoč uporabnikom v primeru zlorabe pri ponudniku internetnih storitev vsekakor zahteva zaposlitev za polni delovni čas za enega ali (v večini primerov) več zaposlenih za polni delovni čas.

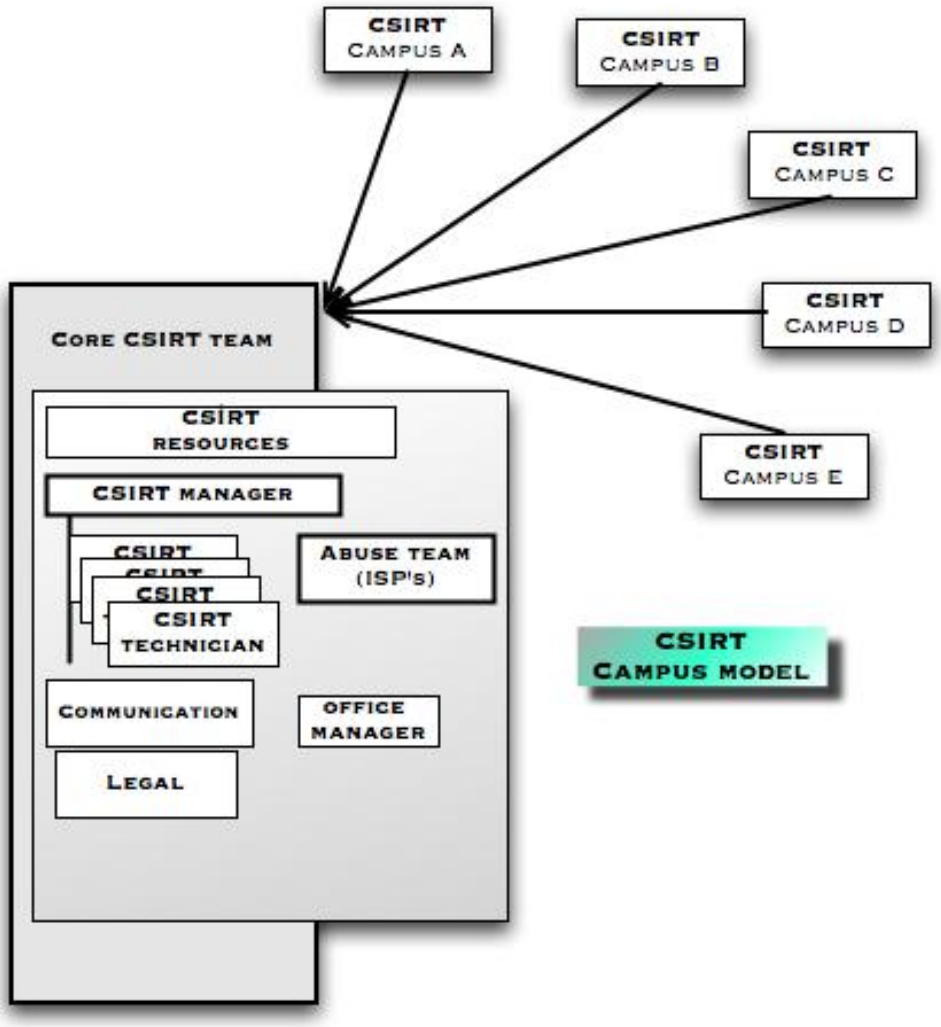


Slika 6 Organizacijski model vgraditve

6.2.3 Model kampusa

Kot je razvidno že iz imena samega, model kampusa prevzemajo predvsem akademske in raziskovalne skupine CSIRT. Večino akademskih in raziskovalnih organizacij sestavljajo različne univerze in kampusi, ki so na različnih lokacijah, po vsej regiji ali celo po vsej državi (kot v primeru omrežij NREN, nacionalnih raziskovalnih omrežij). Običajno so te organizacije med seboj neodvisne, pogosto pa imajo tudi svojo skupino CSIRT. Te skupine CSIRT so običajno organizirane pod okriljem „matere“ ali osnovne skupine CSIRT. Ta osnovna skupina CSIRT skrbi za usklajevanje in zunanjemu svetu predstavlja edino kontaktno točko. V večini primerov bo osnovna skupina CSIRT prav tako zagotavljala storitve osnovne skupine, hkrati pa ustreznim kampusom skupine CSIRT posreduje tudi informacije o incidentih.

Nekatere skupine CSIRT si z drugimi skupinami CSIRT v kampusih izmenjujejo storitve osnovne skupine CSIRT, kar ima za posledico manjšo obremenjenost osnovne skupine CSIRT.



Slika 7 Model kampusa

6.2.4 Prostovoljni model

Ta organizacijski model opisuje skupino ljudi (strokovnjakov), ki so se združili, da bi si med sabo (ali drugim) pomagali ali nudili podporo na prostovoljni osnovi. Gre za ohlapno povezano skupnost, ki je zelo odvisna od motiviranosti sodelujočih.

Ta model je na primer prevzela skupnost WARP[13].

6.3 Zaposlovanje ustreznega osebja

Naslednji korak po sprejetju odločitve glede storitev in ravni zagotovljene podpore ter po izbiri organizacijskega modela je iskanje ustreznega števila usposobljenih ljudi, primernih za to delo.

Skoraj nemogoče je navesti dejanske zneske sredstev, potrebnih za tehnično osebje, vseeno pa so se naslednje ključne vrednosti izkazale kot dobri približki:

- Za zagotavljanje dveh ključnih storitev distribucije svetovalnih oglasnih desk kot tudi reševanje incidentov: najmanj **4** FTE.
- Za celotno storitev skupine CSIRT v času uradnih ur in vzdrževanje sistemov: najmanj **6 do 8** FTE.
- Za polno zasedeno izmeno 24 ur na dan, 7 dni v tednu (2 izmeni v času izven uradnih ur) približno **12** FTE.

V te številke so vključeni tudi dodatki za primere bolezni, praznikov itd. Prav tako je treba preveriti lokalne kolektivne pogodbe o zaposlitvi. Če ljudje delajo izven uradnih ur, ima lahko to za posledico dodatne stroške v obliki dodatnih plačanih nadur.

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

Sledi kratek pregled ključnih pristojnosti tehničnih strokovnjakov v skupini CSIRT.

Splošen opis delovnih nalog tehničnega osebja:

Osebne lastnosti

- prilagodljivost, kreativnost in dober smisel za delo v skupini,
- dobra analitična znanja,
- sposobnost posredovanja težkih tehničnih zadev z enostavnimi besedami,
- dober občutek za zaupnost in delo v skladu s postopkovnimi vprašanji,
- dobre organizacijske sposobnosti,
- odpornost na stres,
- visoka stopnja pismenosti in komunikativnosti,
- odprtost in pripravljenost na učenje.

Tehnična usposobljenost

- dobro poznavanje internetne tehnologije in protokolov,
- poznavanje sistemov Linux in Unix (odvisno od opreme pri odjemalcih),
- poznavanje sistemov Windows (odvisno od opreme pri odjemalcih),
- poznavanje mrežne infrastrukture (usmerjevalnik, stikala, DNS, posredovalni strežnik, strežnik za elektronsko pošto itd.),
- poznavanje spletnih aplikacij (SMTP, protokolov HTTP, FTP, telnet, SSH itd.),
- poznavanje varnostnih groženj (porazdelitvena onesposobitev storitev, lažno predstavljanje, uničevanje, vohunjenje itd.),
- znanje na področju ocenjevanja tveganj in praktična uporaba.

Dodatne lastnosti

- pripravljenost do dela 24 ur na dan, 7 dni v tednu ali na poziv (odvisno od modela zagotavljanja storitev),
- največja oddaljenost (razpoložljivost v primeru izrednih razmer v pisarni; najdaljši čas potovanja),
- stopnja izobrazbe,
- delovne izkušnje na področju varnosti IT.

Navidezna CSIRT (4. korak)

Priprava poslovnega načrta

Finančni model

Na osnovi dejstva, da ima podjetje vzpostavljeno e-poslovanje 24 ur na dan, 7 dni v tednu, prav tako pa tudi oddelek IT, ki deluje 24 ur na dan, 7 dni v tednu, je sprejeta odločitev, da bo zagotavljalo vse storitve v uradnem času, izven uradnih ur pa delo na poziv. Odjemalcem bodo storitve na voljo brezplačno, v fazi priprave in ocenjevanja pa se bo preučila možnost zagotavljanja storitev zunanjim strankam.

Model prihodkov

Skupina CSIRT se bo v začetni in poskusni fazi financirala prek podjetja gostitelja. V poskusni fazi in fazi ocenjevanja bodo proučeni tudi dodatni viri financiranja, vključno z možnostjo prodaje storitev zunanjim strankam.

Organizacijski model
Ker je organizacija gostiteljica majhno podjetje, je bil izbran model vgraditve.
V uradnih urah bodo osnovne storitve (distribucija varnostnih nasvetov in reševanje/usklajevanje incidentov) zagotavljale tri osebe.

V oddelku IT so že zaposlene osebe z ustreznimi izkušnjami. S tem oddelkom se sklene sporazum, tako da lahko nova skupina CSIRT po potrebi zahteva podporo za posamezne projekte. Prav tako lahko uporablja drugo linijo tehnikov na poziv.
Osnovna skupina CSIRT bo sestavljena iz štirih članov s polnim delovnim časom in petih dodatnih članov skupine CSIRT. Eden izmed teh prav tako sodeluje v izmenah.

Osebje
Vodja skupine CSIRT ima izkušnje na področju varnosti in podpore na prvi in drugi stopnji, prav tako pa je opravljal delo na področju kriznega upravljanja. Ostali trije člani skupine so strokovnjaki za varnost. Člani skupine CSIRT, ki niso zaposleni za poln delovni čas in so iz oddelka IT, so strokovnjaki na področju infrastrukture podjetja.

6.4 Uporaba pisarne in pisarniška oprema

Ker oprema in izkoriščanje pisarniškega prostora ter fizična varnost predstavljajo zelo splošno temo, v tem dokumentu ni mogoče navesti nobenih podrobnih opisov. To poglavje daje kratek pregled tega področja.

Več informacij o fizični varnosti lahko najdete na:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

„Utrjevanje stavbe“
Ker skupina CSIRT običajno ravna z zelo občutljivimi informacijami, je dobra praksa, da prevzame nadzor nad fizično varnostjo pisarne. To bo zelo odvisno od obstoječih prostorov in infrastrukture ter obstoječe politike varovanja informacij podjetja gostitelja.

Vlade ravnajo na primer z razvrstitvenimi shemami in so zelo stroge na področju ravnanja z zaupnimi informacijami. Pri vašem podjetju ali ustanovi preverite lokalna pravila in politike.

Nova skupina CSIRT se običajno zanaša na sodelovanje z organizacijo gostiteljico za pridobivanje informacij o lokalnih pravilih, politikah in drugih pravnih vprašanjih.

Ta dokument ne pokriva podrobnega opisa vse opreme in varnostnih ukrepov, ki bodo potrebni. Spodaj boste našli kratek seznam osnovne infrastrukture, potrebne za vašo skupino CSIRT:

Splošna pravila glede stavbe
- Uporaba nadzora dostopa.
- Prostori skupine CSIRT naj bodo dostopni samo osebju skupine CSIRT.
- Nadzor prostorov in vhodov s kamero.
- Arhiviranje zaupnih informacij v omaricah s ključavnico ali sefu.
- Uporaba varnih sistemov IT.

Splošna pravila za opremo IT
- Uporaba opreme, ki jo lahko osebje podpira.
- Okrepitev vseh sistemov.
- Nameščanje popravkov in posodobitev na vseh sistemih preden so povezani z internetom.
- Uporaba varnostne programske opreme (požarni zid, različna programska oprema za odkrivanje virusov, programska oprema za odkrivanje vohunskega programja itd.).

Vzdrževanje komunikacijskih kanalov
- Spletno mesto, namenjeno javnosti.
- Zaprta območja za člane na spletnem mestu.
- Spletni forumi, kjer je mogoče prijaviti incidente.
- Elektronska pošta (podpora PGP/GPG/S/MIME).
- Programska oprema za poštne sezname.
- Namenska telefonska številka, ki je odjemalcem na voljo:
  - Telefon
  - Telefaks
  - SMS

Sistem(i) spremljanja evidenc
- Podatkovna baza s kontakti, ki vsebuje podrobne informacije o članih skupine, drugih skupinah itd.
- Orodja za CRM.
- Sistem reševanja incidentov.

Uporaba „korporativnega videza“ od samega začetka za
- oblikovanje standardnih elektronskih sporočil in svetovalnih oglasnih desk,
- „tradicionalna“ pisma v papirni obliki,
- mesečna ali letna poročila,
- obrazec za prijavo incidenta.

Druga vprašanja
- Zagotovljeni neobičajni načini komuniciranja v primeru napadov.
- Predvidevanje redundance pri povezovanju na internet.

Več informacij o posebnih orodjih skupine CSIRT je mogoče najti v poglavju *8.5 Orodja, ki so na voljo skupini CSIRT.*

6.5 Razvoj informacijske varnostne politike

Vaša informacijska varnostna politika bo odvisna od vrste skupine CSIRT. Poleg tega, da opisujejo želeno stanje operacijskih in upravnih procesov in postopkov, mora biti takšna politika usklajena tudi z zakonodajo in standardi, predvsem v zvezi z odgovornostjo skupine CSIRT. Skupina CSIRT je običajno vezana na državne zakone in predpise, ki se pogostokrat izvajajo v okviru evropske zakonodaje (običajno v direktivah) in drugih mednarodnih sporazumih. Ni nujno, da so standardi neposredno zavezujoči, lahko pa jih zahtevajo ali priporočajo zakonodaja ali predpisi.

Spodaj lahko najdete kratek seznam morebitnih zakonov in politik:

Nacionalni
- Različni zakoni o informacijski tehnologiji, telekomunikaciji, medijih.
- Zakoni o varovanju in zaupnosti podatkov.
- Zakoni in predpisi o hranjenju podatkov.
- Zakoni o financah, računovodstvu in korporativnem upravljanju.
- Kodeksi ravnanja za upravljanje družb in upravljanje informacijske tehnologije.

Evropski
- Direktiva Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis.
- Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov in Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah).
- Direktive o elektronskih komunikacijskih omrežjih in storitvah (2002/19/ES do 2002/22/ES).
- Direktive o pravu družb (npr. Osma direktiva Sveta o pravu družb).

Mednarodni
- Sporazum Basel II (predvsem v povezavi z obvladovanjem operativnih tveganj).
- Konvencija Sveta Evrope o računalniškem kriminalu.
- Konvencija Sveta Evrope o človekovih pravicah (člen 8 o zasebnosti).
- Mednarodni računovodski standardi (MRS; do določene mere predvideva IT nadzor).

Standardi
- Britanski standard BS 7799 (varnost informacij);
- Mednarodni standardi ISO2700x (Upravljavski sistem za varovanje informacij);
- Nemški IT-Grundschutzbuch, francoski EBIOS in druge nacionalne različice.

S svojim pravnim svetovalcem se posvetujte, ali vaša skupina CSIRT deluje v skladu z državno in mednarodno zakonodajo.

Najosnovnejša vprašanja, na katera morate odgovoriti v politikah za ravnanje z informacijami, so:

- Kako so vhodne informacije „označene“ ali „razvrščene“?
- Kako se ravna z informacijami, predvsem v zvezi z ekskluzivnostjo?
- Kateri ukrepi se izvajajo pri razkrivanju informacij, predvsem pri posredovanju informacij, ki se nanašajo na incident, drugim skupinam ali na druge lokacije?
- Ali je treba pri ravnanju z informacijami upoštevati pravne vidike?
- Ali obstaja politika glede uporabe šifriranja za zaščito ekskluzivnosti in celovitosti v arhivih in/ali podatkovnih komunikacijah, predvsem pri elektronski pošti?
- Ali ta politika vsebuje možne pravne mejne pogoje, kot so garancijske listine ali izvršljivost dešifriranja v primeru tožb?

Navidezna CSIRT (5. korak)

Oprema prostorov in njihova lokacija

Ker ima podjetje gostitelj že vzpostavljeno učinkovito fizično varnost, je nova skupina CSIRT s tega vidika dobro pokrita. V primeru izjemnih razmer je zagotovljena „vojna soba“, ki omogoča usklajevanje. Za občutljivo dokumentacijo in šifrirano gradivo se zagotovi sef. Vzpostavljena je bila ločena telefonska linija, vključno s telefonsko centralo, kar omogoča delovanje klicnega centra v uradnih urah in službenega mobilnega telefona „na poziv“ za čas izven uradnih ur z isto telefonsko številko.

Za objavo informacij, povezanih s skupino CSIRT, je mogoče uporabiti tudi obstoječo opremo in spletno stran podjetja. Vzpostavljen in vzdrževan je poštni seznam z omejenim delom za komunikacijo med člani skupine in drugimi skupinami. Vse kontaktne informacije o osebju so shranjene v podatkovni bazi, izpis teh podatkov pa se hrani v sefu.

Ureditev

Ker je bila skupina CSIRT vzpostavljena znotraj podjetja z obstoječimi politikami varnosti informacij, so bile ustrezne politike za skupino CSIRT pripravljene s pomočjo pravnega svetovalca podjetja.

6.6 Iskanje sodelovanja z drugimi skupinami CSIRT in morebitnimi državnimi pobudami.

V tem dokumentu smo že večkrat omenili obstoj drugih pobud CSIRT in močno potrebo po sodelovanju med njimi. Čim prejšnje kontaktiranje drugih skupin CSIRT, ki omogoča pridobitev potrebnih stikov s skupnostmi CSIRT, je dobra praksa. Druge skupine CSIRT so običajno pripravljene pomagati novo ustanovljenim skupinam.

Seznam dejavnosti skupin CERT v Evropi [14] agencije ENISA predstavlja zelo dobro mesto za iskanje drugih skupin CSIRT v državi ali za iskanje sodelovanja s skupinami CSIRT na državni ravni.

Za pomoč pri iskanju primernega vira informacij o skupinah CSIRT se obrnite na strokovnjake za CSIRT agencije ENISA:

CERT-Relations@enisa.europa.eu

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

Sledi pregled dejavnosti, ki potekajo v skupnosti CSIRT. Podrobnejše opise in dodatne informacije lahko najdete v *Seznamu*.

Evropska pobuda CSIRT

TF-CSIRT[15]
Delovna skupina TF-CSIRT spodbuja sodelovanje med skupinami za reševanje varnostnih incidentov (skupine CSIRT) v Evropi. Glavni cilji te delovne skupine so zagotovitev foruma za izmenjavo izkušenj in znanja, vzpostavitev poskusnih storitev za skupnost evropskih skupin CSIRT in zagotavljaje pomoči pri vzpostavljanju novih skupin CSIRT.

Glavni cilji delovne skupine so:
- Zagotovitev foruma za izmenjavo izkušenj in znanja.
- Vzpostavitev poskusnih storitev za skupnost evropskih skupin CSIRT.
- Spodbujanje skupnih standardov in postopkov pri reševanju varnostnih incidentov.
- Zagotavljanje pomoči pri vzpostavljanju novih skupin CSIRT in usposabljanju osebja skupin CSIRT.
- Dejavnosti delovne skupine TF-CSIRT so usmerjene na Evropo in sosednje države, v skladu z referenčnimi pogoji, ki jih je 15. septembra 2004 odobril tehnični odbor TERENA.

Globalna pobuda CSIRT

FIRST[16]
FIRST je organizacija, ki je vodilna v svetu na področju reševanja incidentov. Skupinam za reševanje incidentov članstvo v organizaciji FIRST omogoča učinkovitejše reševanje varnostnih incidentov - tako reaktivnih, kot tudi proaktivnih.

Organizacija FIRST združuje različne skupine za reševanje varnostnih incidentov iz različnih vladnih, komercialnih in izobraževalnih organizacij. Cilj organizacije FIRST je okrepiti sodelovanje in usklajevanje na področju preprečevanja incidentov, spodbujati hitro reševanje incidentov in olajšati izmenjavo informacij med člani in širšo skupnostjo.

Poleg zaupanja vrednega omrežja, ki ga organizacija FIRST predstavlja v globalni skupnosti za reševanje incidentov, zagotavlja tudi storitve z dodano vrednostjo.

Navidezna CSIRT (6. korak)
Iskanje sodelovanja S pomočjo seznama agencije ENISA je bilo mogoče hitro najti nekaj skupin CSIRT v isti državi in z njimi tudi navezati stike. Za novega voditelja skupine je bil organiziran obisk ene izmed teh skupin. Seznanil se je z državnimi dejavnostmi skupine CSIRT in se udeležil sestanka. Ta sestanek je bil več kot koristen pri zbiranju primerov delovnih metod in pridobivanju podpore s strani drugih dveh skupin.

[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 Spodbujanje poslovnega načrta

Do sedaj smo opravili naslednje korake:

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.
2. Kateremu sektorju bo skupina CSIRT zagotavljala storitve?
3. Katere storitve lahko CSIRT zagotavlja svojim odjemalcem.
4. Analiziranje okolja in odjemalcev.
5. Določitev poslanstva.
6. Priprava poslovnega načrta.
    a. Priprava finančnega modela.
    b. Določitev organizacijske strukture.
    c. Začetek zaposlovanja osebja.
    d. Izraba in opremljanje pisarne.
    e. Razvoj politike informacijske varnosti.
    f. Iskanje partnerjev za sodelovanje.

>> Naslednji korak je prenos zgoraj navedenega v projektni načrt in začetek dela!

Priprava poslovnega primera predstavlja dober začetek pri opredelitvi projekta. Ta poslovni primer bo služil kot osnova za projektni načrt, prav tako pa se bo uporabljal pri pridobivanju podpore s strani vodstva ter proračuna in drugih virov.

Nenehno poročanje vodstvu se je prav tako izkazalo kot zelo koristno pri visoki osveščenosti glede varnostnih problemov IT in pri zagotavljanju stalne podpore za lastno skupino CSIRT.

Priprava poslovnega primera se začne z analiziranjem problemov in priložnosti, pri čemer se uporabljajo analitični modeli, opisani v poglavju 5.3 *Analiza odjemalcev*, in iskanjem stikov z morebitnimi odjemalci.

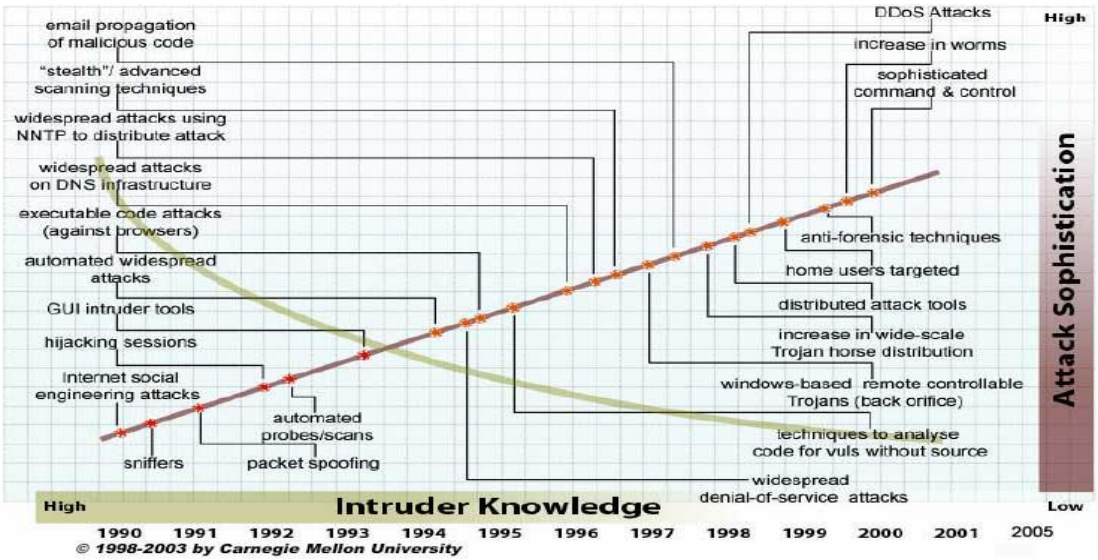
Kot je bilo že prej navedeno, je pri vzpostavitvi skupine CSIRT treba upoštevati veliko dejstev. Najbolje je sproti prilagajati zgoraj navedeno gradivao potrebam skupine CSIRT, ko se ta razvija.

Prav tako šteje kot dobra praksa poročanje vodstvu in s tem posodabljanje posameznih primerov z uporabo nedavnih člankov iz časopisa ali interneta in navajanje razlogov, zakaj so storitve skupine CSIRT in notranje usklajevanje incidentov ključnega pomena za zaščito poslovnih sredstev. Prav tako je treba jasno navesti, da le nenehna podpora na področju zadev, ki se nanašajo na varnost IT, vodi do stabilnega podjetja, predvsem pri podjetjih ali ustanovah, ki so odvisne od informacijske tehnologije.

(Poznana fraza Bruca Schneierja to le še poudarja: *„Varnost ni izdelek, temveč proces[17]!“)*

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

Znano orodje za ponazoritev varnostnih problemov je naslednji graf, ki ga je posredovala skupina CERT/CC:



Slika 8 Znanje vsiljivca v nasprotju z dovršenostjo napada (vir CERT-CC[18])

Prikazuje smernice na področju varnosti IT, predvsem zmanjšanje potrebnega znanja za izvedbo vse bolj dovršenih napadov.

Naslednja stvar, ki jo je treba poudariti, je nenehno skrajševanje časa med razpoložljivostjo posodobitev programske opreme zaradi ranljivosti in začetkom izvajanja napadov na njih:

Popravek ->	**Zloraba pomanjkljivosti**	**Stopnja širjenja**	
Nimda:	11 mesecev	Code red:	Dnevi
Slammer:	6 mesecev	Nimda:	Ure
Nachi:	5 mesecev	Slammer:	Minute
Blaster:	3 tedne		
Witty:	1 dan (!)		

Prav tako predstavljajo dobro predstavitev zbrani podatki o incidentih, morebitne izboljšave in pridobljene izkušnje.

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

7.1 Opis poslovnega načrta in ukrepanje s strani vodstva

Predstavitev za vodstvo, vključno s predstavitvijo skupine CSIRT same, še ne pomeni poslovnega primera, če pa je izvedena na ustrezen način, pa lahko skupina CSIRT pridobi podporo s strani vodstva v večini primerov. Seveda pa na poslovni primer ne moremo gledati le kot na odločitev vodstva, ampak ga je mogoče uporabiti tudi za komunikacijo s skupino in odjemalci. Pojem poslovni primer zveni precej komercialno in se zdi precej odmaknjen od vsakodnevne prakse skupine CSIRT, vendar daje dobro izhodišče in usmeritve pri vzpostavljanju skupine CSIRT.

Pri pripravi dobrega poslovnega primera lahko uporabite odgovore na naslednja vprašanja (gre za hipotetične primere, ki se uporabljajo samo za ponazoritev. „Pravi“ odgovori so zelo odvisni od „pravih“ okoliščin).

- V čem je problem?
- Kaj nameravate doseči pri svojih odjemalcih?
- Kaj se bo zgodilo, če ne boste ukrepali?
- Kaj se bo zgodilo, če boste ukrepali?
- Koliko bo to stalo?
- Kakšne bodo koristi?
- Kdaj začeti in kdaj bo končano?

V čem je problem?
Ideja o vzpostavitvi skupine CSIRT se v večini primerov poraja, ko varnost IT postane temeljni del glavne dejavnosti podjetja ali ustanove in ko varnostni incidenti IT začnejo ogrožati poslovanje, zaradi česar varnostne omejitve postanejo del običajnega delovanja podjetja.

Večina podjetij ali ustanov ima reden oddelek za podporo ali službo za podporo uporabnikom, vendar reševanje varnostnih incidentov v večini primerov ni ustrezno, prav tako pa ni strukturirano tako, kot bi moralo biti. V večini primerov sta za delovanje na področju varnostnih incidentov potrebna posebno znanje in pazljivost. Pozitivne lastnosti ima tudi bolj strukturiran pristop, ki hkrati tudi zmanjšuje poslovna tveganja in škodo, ki bi jo utrpelo podjetje.

V večini primerov je težava v tem, da ni primernega usklajevanja in da se za reševanje incidentov ne uporablja obstoječe znanje, ki bi lahko preprečilo nastanek teh incidentov v prihodnje, prav tako pa bi preprečilo tudi morebitne finančne izgube in/ali škodo za ugled ustanove.

Kaj nameravate doseči pri svojih odjemalcih?
Kot je bilo razloženo že prej, bo vaša skupina CSIRT zagotavljala storitve za svoje odjemalce in jim pomagala pri reševanju varnostnih incidentov in težav, povezanih z informacijsko tehnologijo. Pri tem so dodatni cilji dviganje ravni poznavanja varnosti IT in vzpostavljanje kulture zavedanja pomena varnosti.

Ta kultura si prizadeva za proaktivne in preventivne ukrepe, ki se izvajajo že od samega začetka in s tem zmanjšujejo operativne stroške.

Uvedba te kulture sodelovanja in pomoči v podjetje ali ustanovo lahko v večini primerov spodbudi učinkovitost.

Kaj se bo zgodilo, če ne boste ukrepali?

Nestrukturiran način obravnavanja varnosti IT lahko ima za posledico dodatno škodo, negativno pa lahko vpliva tudi na ugled ustanove. Druge posledice so lahko v obliki finančnih izgub in pravnih posledic.

Kaj se bo zgodilo, če boste ukrepali?

Dvignila se bo osveščenost glede pojavljanja varnostnih problemov. To bo v pomoč pri učinkovitejšem reševanju teh problemov in preprečevanju izgub v prihodnje.

Koliko bo to stalo?

Glede na organizacijski model bodo strošek plače članov skupine CSIRT in organizacije, opreme, orodja in licenc programske opreme.

Kakšne bodo koristi?

Glede na podjetje in izgube v preteklosti bo zagotovljena večja preglednost postopkov in varnostnih politik, s tem pa bodo zaščitena glavna sredstva podjetja.

Kakšen je časovni načrt?

Za opis vzorčnega projektnega načrta glejte poglavje *12. Opis projektnega načrta*.

Primeri obstoječih poslovnih primerov in pristopov

Navedenih je nekaj primerov poslovnih primerov skupine CSIRT, ki jih je vredno preučiti:

- http://www.cert.org/csirts/AFI_case-study.html
  Vzpostavitev skupine CSIRT v finančni ustanovi: Študija primera

  Namen tega dokumenta je izmenjava izkušenj, ki jih je pridobila finančna ustanova (v tem dokumentu poimenovana kot AFI) pri razvoju in izvedbi načrta, ki se je nanašal na varnostna vprašanja in skupine za reševanje varnostnih incidentov (CSIRT).

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Povzetek poslovnega primera skupine CERT POLSKA (predstavitev v obliki PDF).

- http://www.auscert.org.au/render.html?it=2252
  Vzpostavitev skupine za reševanje incidentov (IRT) je lahko po letu 1990 precej naporno opravilo. Številni ljudje, ki vzpostavljajo IRT, nimajo nobenih izkušenj na tem področju. Ta dokument opisuje vlogo, ki jo lahko ima IRT v skupnosti, in vprašanja, na katera je treba odgovoriti med vzpostavitvijo in po začetku izvajanja operacij. Dokument je lahko uporaben tudi za obstoječe skupine IRT, saj dviga osveščenost o nerešenih vprašanjih.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Študija primera varovanja informacij, zaščita podjetja, avtor: Roger Benton

  Gre za študijo primera o prehodu zavarovalnice na varnostni sistem, ki ga uporablja celotno podjetje. Namen tega priročnika je zagotoviti pot, ki ji je mogoče slediti pri vzpostavljanju varnostnega sistema ali prehodu nanj. V začetku se je kot edini mehanizem za nadzor dostopa do podatkov o podjetju uporabljal samo enostaven varnostni sistem na spletu. Izpostavljenost je bila velika – izven spletnega okolja ni bilo nobenega celostnega nadzora. Vsakdo, ki je imel nekaj osnovnega znanja o programiranju, je lahko dodajal, spreminjal in/ali brisal podatke.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  E-varnostna strategija podjetja Marriott: Poslovno IT sodelovanje.

  Po izkušnjah Chrisa Zoladza pri Marriott International, Inc. je e-poslovna varnost proces in ne projekt. Takšno sporočilo je Zoladz posredoval tudi na nedavni konferenci o e-varnosti na Expo v Bostonu, ki jo je sponzorirala skupina Intermedia Group. Zoladz, podpredsednik oddelka za varovanje informacij pri podjetju Marriott, pripravlja poročila prek pravnega oddelka, čeprav sam ni odvetnik. Njegova naloga je opredeliti, kje so shranjene najbolj občutljive poslovne informacije podjetja Marriott in kako se gibajo v in izven podjetja. Marriott je za tehnično infrastrukturo, ki zagotavlja varnost, vzpostavil ločeno odgovornost, ki je bila podeljena snovalcem varnosti IT.

Navidezna CSIRT (7. korak)
Spodbujanje poslovnega načrta Sprejeta je odločitev o zbiranju podatkov iz zgodovine podjetja. S tem bo možen statistični pregled nad razmerami na področju varnosti IT. To zbiranje se bo nadaljevalo tudi po začetku delovanja skupine CSIRT, da bi na ta način statistični podatki ostali posodobljeni. Opravljeno je bilo tudi posvetovanje z drugimi nacionalnimi skupinami CSIRT o njihovih poslovnih primerih. Te skupine so pripravile nekaj diapozitivov z informacijami o nedavnih dogodkih, povezanih z incidenti na področju varnosti IT, in o stroških, ki so jih povzročili ti incidenti. V tem primeru navidezne skupine CSIRT vodstva ni bilo potrebno prepričevati o pomembnosti poslovnih procesov IT in prav zaradi tega ni bilo težko pridobiti dovoljenja za izvedbo prvega koraka. Pripravljena sta bila poslovni primer in projektni načrt, vključno z oceno stroškov vzpostavitve in stroškov, povezanih z delovanjem.

8 Primeri operativnih in tehničnih postopkov (potek dela)

Do sedaj smo opravili naslednje korake:

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.
2. Kateremu sektorju bo skupina CSIRT zagotavljala storitve?
3. Katere storitve lahko CSIRT zagotavlja svojim odjemalcem.
4. Analiziranje okolja in odjemalcev.
5. Določitev poslanstva.
6. Priprava poslovnega načrta.
   a. Priprava finančnega modela.
   b. Določitev organizacijske strukture.
   c. Začetek zaposlovanja osebja.
   d. Izraba in opremljanje pisarne.
   e. Razvoj politike informacijske varnosti.
   f. Iskanje partnerjev za sodelovanje.
7. Spodbujanje poslovnega načrta.
   a. Odobritev poslovnega primera.
   b. Priprava projektnega načrta.

>> Naslednji korak je: začetek delovanja skupine CSIRT.

Kakovost in čas, potrebna za posamezen incident ali posamezen primer ranljivosti, je mogoče izboljšati z dobro opredeljenimi poteki dela.

Kot je opisano v okvirih s primeri, bo navidezna CSIRT ponujala osnovne storitve skupine CSIRT:

- Obveščanje in opozorila
- Reševanje incidentov
- Najave

To poglavje vsebuje primere postopkov dela, ki opisujejo osnovne storitve skupine CSIRT. To poglavje prav tako vsebuje informacije o zbiranju informacij iz različnih virov, o njihovi pomembnosti in pristnosti ter o njihovem distribuiranju odjemalcem. To poglavje pa vsebuje tudi primere o najosnovnejših postopkih in posebnem orodju skupine CSIRT.

8.1 Dostop do infrastrukture odjemalcev

Prvi korak je pridobiti informacije o sistemih IT, nameščenih pri odjemalcih. Na ta način lahko skupina CSIRT oceni pomembnost vhodnih informacij in jih pred ponovno distribucijo filtrira ter na ta način prepreči, da bi odjemalce zasula z informacijami, ki za njih sploh niso pomembne.

Dobra praksa je začeti enostavno, na primer z uporabo Excelove preglednice, kot je razvidno iz naslednjega primera:

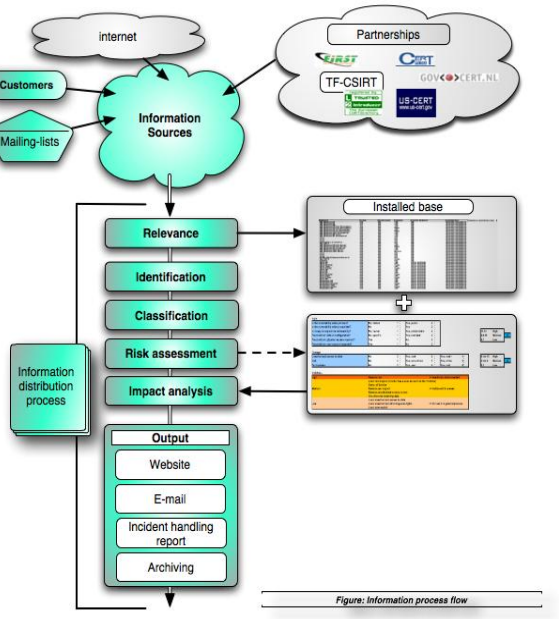
Kategorija	Aplikacija	Programska oprema	Različica	OS	OS različica	Odjemalec
Namizje	Pisarna	Excel	x-x-x	Microsoft	XP-prof	A
Namizje	Brskalnik	IE	x-x-	Microsoft	XP-prof	A
Omrežja	Usmerjevalnik	CISCO	x-x-x	CISCO	x-x-x-	B
Strežnik	Strežnik	Linux	x-x-x	L-distro	x-x-x	B
Storitve	Spletni strežniki	Apache		Unix	x-x-x	B

S filtriranjem v programski opremi Excel je mogoče zelo enostavno izbrati ustrezno programsko opremo in ugotoviti, kateri odjemalec uporablja katero programsko opremo.

8.2 Priprava alarmov, opozoril in najav

Pri pripravi alarmov, opozoril in najav se uporablja isti potek dela:

- Pridobivanje informacij;
- Ocenjevanje informacij glede pomembnosti in virov;
- Ocenjevanje tveganj, ki temelji na pridobivanju informacij;
- Distribucija informacij;



Slika 9 Potek obdelave informacij

Ta pretok dela bo podrobneje opisan v naslednjih odstavkih.

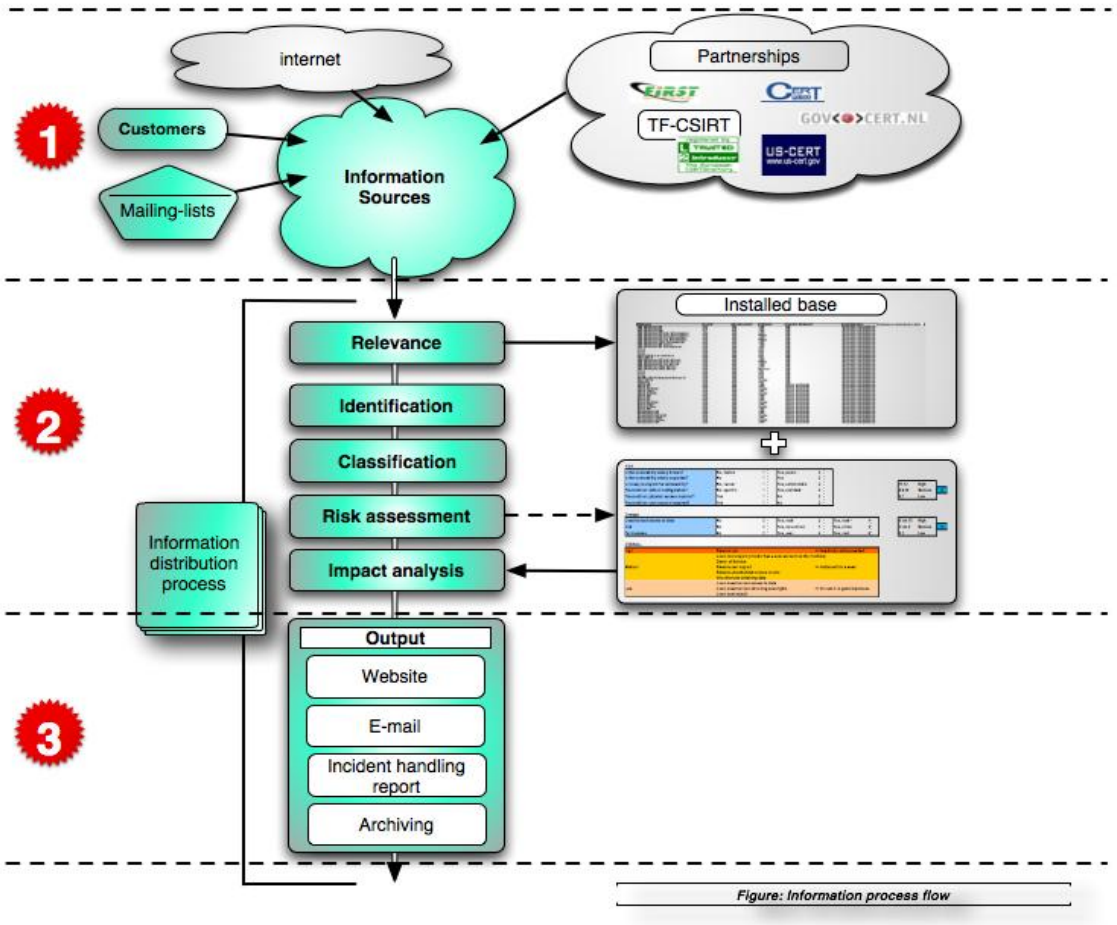


Figure: Information process flow

1. korak: Pridobivanje informacij o ranljivosti

Običajno obstajata dve glavni vrsti informacijskih virov, ki zagotavljajo informacije, kot vhodne podatke pri storitvah:

- Informacije o ranljivosti (vaših) sistemov IT.
- Poročila o incidentih.

Na voljo so številni javni in zaprti viri za pridobivanje informacije o ranljivosti, ki so odvisni od vrste podjetja in infrastrukture IT:

- javni in zaprti seznami poštnih naslovov,
- informacije o ranljivosti izdelkov s strani dobavitelja,
- spletna mesta,
- informacije na internetu (Google, itd...),
- javna in zasebna partnerstva, ki zagotavljajo informacije o ranljivosti (FIRST, TF-CSIRT, CERT-CC, US-CERT….).

Vse te informacije prispevajo k stopnji poznavanja posameznih ranljivosti v sistemih IT.

Kot je bilo že navedeno, je na internetu na voljo veliko dobrih in enostavno dostopnih virov o varnostnih informacijah. Začasna delovna agencija ENISA „storitve CERT“ v času sestavljanja tega dokumenta za leto 2006 pripravlja celovitejši seznam, ki naj bi bil končan do konca leta 2006[19].

2. korak: Presoja informacij in ocenjevanje tveganja

V tem koraku bo pripravljena analiza vpliva posameznih ranljivosti, ki jim je izpostavljena infrastruktura IT odjemalca.

Identifikacija
Vir vhodnih informacij o ranljivosti mora biti vedno določen, prav tako pa je treba pred posredovanjem kakršnih koli informacij odjemalcem ugotoviti ali je ta vir zanesljiv. Sicer lahko pride do napačnega obveščanja, kar lahko vodi do nepotrebnih motenj v poslovnih procesih, v končni fazi pa to škoduje tudi ugledu skupin CSIRT.

[19] Začasne storitve DS CERT: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Naslednji postopek vsebuje primer identifikacije pristnosti sporočila:

Postopek za identifikacijo pristnosti sporočila in njegovega vira

Splošni kontrolni seznam
1. Ali je vir poznan in kot takšen registriran?
2. Ali so informacije posredovane po običajnem kanalu?
3. Ali vsebuje „nenavadne“ informacije, ki vzbujajo občutek, „da je nekaj narobe“?
4. Sledite svojemu občutku, če obstaja dvom o informacijah, ne ukrepajte takoj, temveč ponovno preverite!

E-pošta – viri
1. Ali organizacija pozna naslov vira in je naveden na seznamu virov?
2. Ali je podpis PGP pristen?
3. Kadar ste v dvomu, preverite celotno glavo sporočila.
4. Kadar ste v dvomih, za preverjanje domene pošiljatelja uporabite „nslookup“ ali „dig“[20].

WWW – Viri
1. Pri dostopanju do varnih spletnih mest (http://) preverite certifikate v brskalnikih.
2. Preverite vir vsebine in veljavnost (tehnično).
3. Kadar ste v dvomih, ne klikajte na povezave in na računalnik ne prenašajte nobene programske opreme.
4. Kadar ste v dvomih domeno preverite z orodji „lookup“ in „dig“, pa tudi „traceroute“.

Telefon
1. Pazljivo prisluhnite imenu in priimku.
2. Ali prepoznate glas?
3. Kadar ste v dvomih, vprašajte za telefonsko številko in se dogovorite, da boste klicatelja poklicali nazaj.

Slika 10 Primer postopka identifikacije informacij

Pomembnost
Prej izveden pregled nameščene strojne in programske opreme se lahko uporabi za filtriranje vhodnih občutljivih informacij glede na pomembnost z namenom iskanja odgovora na vprašanja: „Ali odjemalci uporabljajo to programsko opremo?“; „Ali je informacija za njih pomembna?“

Klasifikacija
Nekatere prejete informacije so lahko razvrščene ali označene kot omejene (na primer vhodna poročila o incidentih s strani drugih skupin). Vse informacije je treba obravnavati v skladu z zahtevami pošiljatelja in v skladu z lastno politiko informacijske varnosti. Dobro osnovno pravilo je *„Ne razpošiljajte informacij, če ni jasno, da so temu namenjene. Kadar ste v dvomih, pošiljatelja povprašajte za dovoljenje“*.

[20] Orodja za preverjanje identitete v CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Ocena tveganja in analize vpliva
Za ocenjevanje tveganja in posledic (potencialne) ranljivosti obstajajo številne metode.

Tveganje je opredeljeno kot potencialna priložnost, da je mogoče izkoristiti ranljivost. Obstajajo številni pomembni dejavniki (med drugimi):

- Ali je ranljivost dobro poznana?
- Ali je ranljivost močno razširjena?
- Ali je ranljivost mogoče izkoristiti na enostaven način?
- Ali gre za ranljivost, ki jo je mogoče izkoristiti z oddaljenega mesta?

Vsa ta vprašanja pripomorejo k boljšemu občutku glede resnosti ranljivosti.
Zelo enostaven pristop za izračunavanje tveganja predstavlja naslednja formula:

Vpliv = tveganje X potencialna škoda

Potencialna škoda je lahko:

- nepooblaščen dostop do podatkov,
- zavrnitev storitev (DOS),
- pridobivanje ali razširjanje uporabniških pravic.

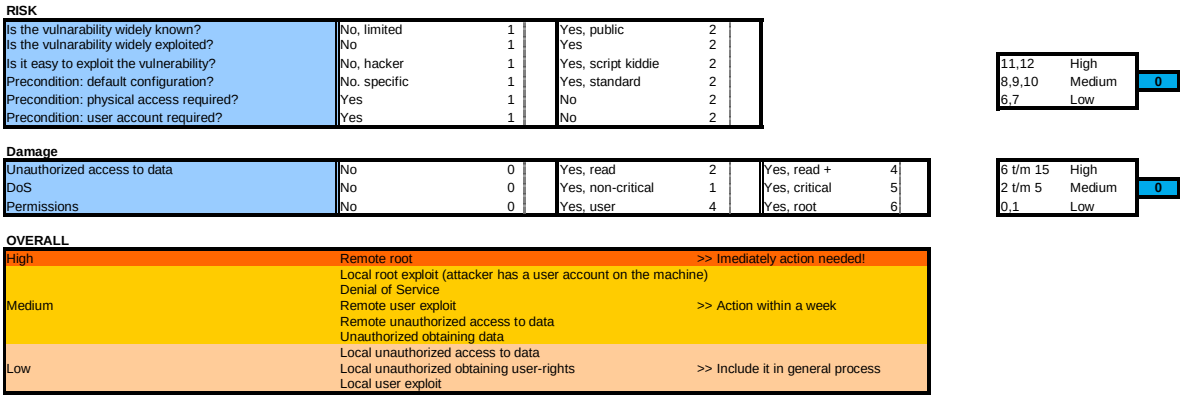
(Podrobnejše razvrstitvene sheme lahko najdete na koncu tega poglavja).

Z navajanjem odgovorov na ta vprašanja je mogoče doprinesti k svetovanju in s tem obveščati o potencialnih tveganjih in škodi. Pogostokrat se uporabljajo preprosti pojmi kot so NIZKO, SREDNJE in VISOKO.

Druge, celovitejše sheme za ocenjevanje tveganj so:

Shema ocenjevanja GOVCERT.NL[21]

Nizozemska vladna skupina CSIRT GOVCERT.NL je ob začetku delovanja skupine Govcert.nl razvila matrico za ocenjevanje tveganj in jo še vedno prilagaja najnovejšim smernicam.



Slika 11 Shema ocenjevanja GOVCERT.NL

Opis običajnega formata svetovanja EISPP[22]

Evropski program za spodbujanje varnosti informacij (EISPP) je projekt, ki ga je soustanovila Evropska skupnost znotraj petega okvirnega programa. Namen projekta EISPP je razviti evropski okvir, ki ni namenjen samo izmenjavi znanja na področju varnosti, ampak tudi opredelitvi vsebine in načinov za posredovanje varnostnih informacij malim in srednje velikim podjetjem. Zagotavljanje potrebnih IT varnostnih storitev bo spodbujalo mala in srednje velika podjetja v Evropi, da okrepijo zaupanje in pogostost uporabe e-poslovanja, ki daje širše in boljše priložnosti za nove posle. Program EISPP je vodilni program Evropske komisije na področju oblikovanja evropskega strokovnega omrežja znotraj Evropske unije.

Nemški svetovalni format DAF[23]

DAF je pobuda nemškega združenja CERT in predstavlja osnovi del infrastrukture pri pripravi in izmenjavi varnostnih nasvetov med različnimi skupinami. DAF je predvsem prilagojen potrebam nemških skupin CERT; standard so razvile in ga vzdržujejo skupine CERT-Bund, DFN-CERT, PRESECURE in Siemens-CERT.

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

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

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

3. korak: Distribucija informacij.

Skupina CSIRT lahko glede na želje odjemalcev in svoje komunikacijske strategije izbira med številnimi distribucijskimi metodami:

- spletna mesta,
- e-pošta,
- poročila,
- arhiviranje in raziskave.

Nasveti glede varnosti, ki jih posreduje skupina CSIRT, so vedno sestavljeni na enak način. S tem se bo izboljšala čitljivost, bralec pa bo lahko hitro našel vse pomembne informacije.

Nasvet mora vsebovati vsaj naslednje informacije:

Naslov nasveta ……
Referenčna številka …… **Prizadeti sistemi** **-** …… **-** …… **Ustrezni OS + različice** …… **Tveganje** (visoko-srednje-nizko) …… **Vpliv/potencialna škoda** (visoka-srednja-nizka) …… **Zunanje identifikacijske številke:** (identifikacijske številke običajne ranljivosti in izpostavljenosti, oglasne deske, ki vsebuje ranljivosti) ……
Pregled ranljivosti …… **Vpliv** …… **Rešitev** …… **Opis (podrobnosti)** …… **Priloga** ……

Slika 12 Vzorec sheme svetovanja

Glejte poglavje *10. Primer* za popoln primer nasvetov o varnosti.

8.3 Reševanje incidentov

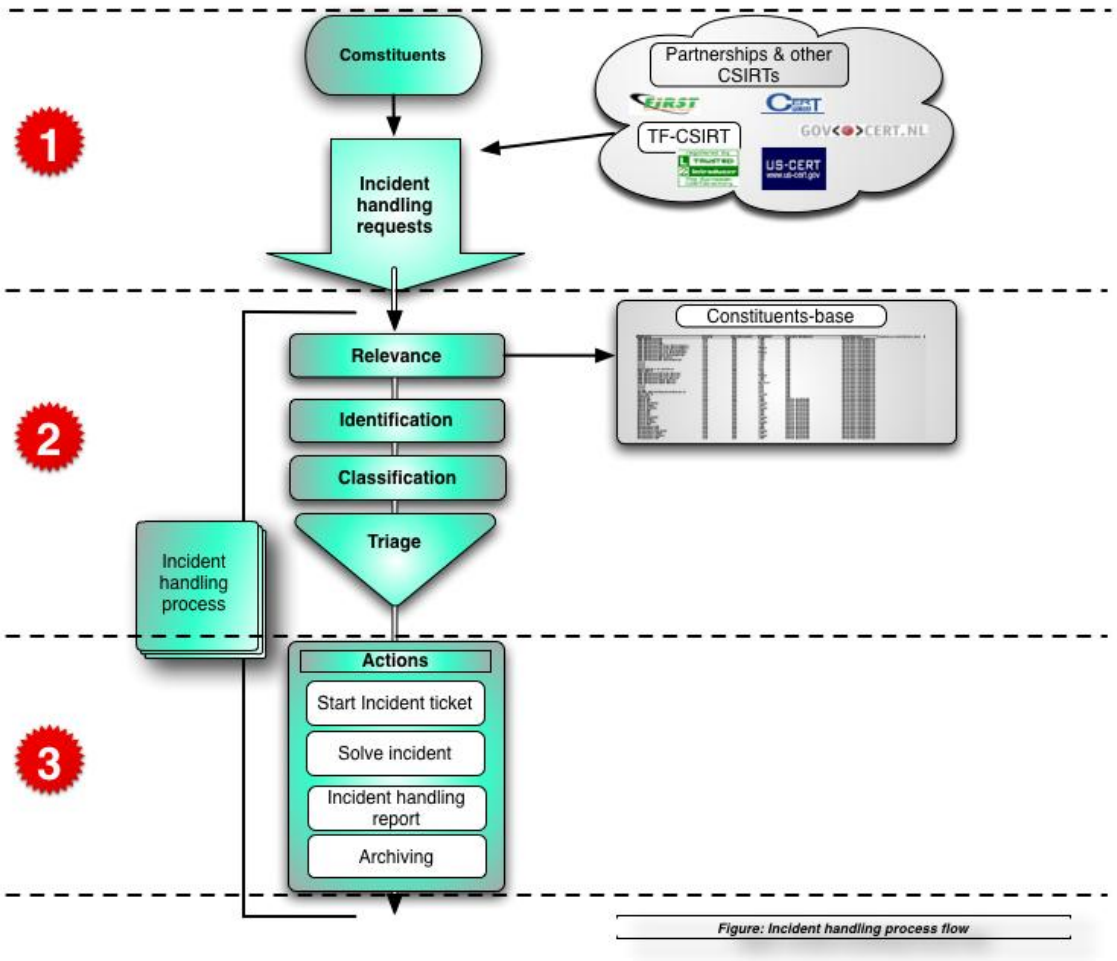
Kot je navedeno v uvodu tega poglavja, je postopek ravnanja z informacijami v času reševanja incidentov zelo podoben postopku, ki se uporablja pri pripravi alarmov, opozoril in najav. Pridobivanje informacij pa se običajno razlikuje, saj je običajen način za pridobivanje podatkov, povezanih z incidenti, prek poročil o incidentih s strani odjemalcev ali drugih skupin ali s prejemanjem povratnih informacij s strani vpletenih strank v času reševanja incidentov. Informacije se običajno izmenjujejo s (šifrirano) elektronsko pošto, včasih pa je treba uporabiti tudi telefon ali telefaks.

Pri prejemanju informacij prek telefona predstavlja dobro prakso takojšnje zapisovanje vseh podrobnosti v obliki zapiska ali z uporabo obrazca za poročanje/reševanje incidentov. Takojšnja (še pred koncem telefonskega pogovora) dodelitev oznake incidenta (če le-ta za ta incident še ne obstaja) je obvezna, prav tako pa jo je treba posredovati tudi poročevalcu na telefonu (ali prek elektronske pošte s povzetkom, ki je poslana naknadno) kot referenco pri nadaljnji komunikaciji.

Preostali del tega poglavja opisuje osnovni postopek reševanja incidenta. Zelo podrobno analizo celotnega procesa upravljanja incidentov in vse povezane poteke dela lahko najdete v dokumentaciji skupine CERT/CC *Določitev procesa upravljanja incidentov za skupine CSIRT*[24].

[24] Določitev procesa upravljanja incidentov: http://www.cert.org/archive/pdf/04tr015.pdf

Pri upravljanju incidentov se v osnovi uporablja naslednji potek dela:



Slika 13 Potek obravnave incidenta

1. korak: Prejemanje poročil o incidentih

Kot je bilo že omenjeno, prejema skupina CSIRT poročila o incidentih prek številnih kanalov, predvsem po elektronski pošti, pa tudi prek telefona ali telefaksa.

Zapisovanje vseh podrobnosti na ustaljen način pri prejemanju poročila o incidentu predstavlja dobro prakso. S tem se zagotovi, da so zabeležene vse bistvene informacije. Sledi vzorčni primer:

OBRAZEC ZA PRIJAVO INCIDENTA

Izpolnite ta obrazec in ga pošljite po telefaksu ali elektronski pošti: ……..
z zvezdico (*) označena polja so obvezna.

Ime, priimek in organizacija
1. Ime in priimek*:
2. Ime organizacije*:
3. Vrsta sektorja:
4. Država*:
5. Mesto:
6. Naslov elektronske pošte*:
7. Telefonska številka*:
8. Drugo:

Prizadeti gostitelj(i)
9. Število gostiteljev:
10. Ime gostitelja in IP naslov*:
11. Funkcija gostitelja*:
12. Časovna cona:
13. Strojna oprema:
14. Operacijski sistem:
15. Prizadeta programska oprema:
16. Prizadete datoteke:
17. Varnost:
18. Ime gostitelja in IP naslov:
19. Protokol/vrata:

Incident
20. Referenčna številka #:
21. Vrsta incidenta:
22. Začetek incidenta:
23. Gre za dlje časa trajajoč incident: DA NE
24. Čas in metoda, s katero je bil incident odkrit:
25. Znane ranljivosti:
26. Sumljive datoteke:
27. Protiukrepi:
28. Podroben opis*:

Slika 14 Vsebina poročila o incidentu

2. korak: Ovrednotenje incidenta

V tem koraku se preveri pristnost in pomembnost incidenta, prav tako pa se ta incident tudi razvrsti.

Identifikacija

Dobra navada je, da preverite, ali je oseba, ki je oddala poročilo, zanesljiva, in ali je ena izmed članov vaše ali partnerske skupine CSIRT, da bi bilo mogoče preprečiti vse nepotrebne ukrepe. Pri tem veljajo podobna pravila, kot so opisana v poglavju *8.2 Priprava alarmov*.

Pomembnost

V tem koraku preverite, če zahteva za reševanje incidenta prihaja s strani odjemalca skupine CSIRT ali če so v prijavljen incident vključeni tudi sistemi odjemalca IT. Če ne velja nič od zgoraj navedenega, se poročilo običajno posreduje ustrezni skupini CISRT[25].

Klasifikacija

V tem koraku se z razvrstitvijo incidenta glede na njegovo resnost pripravi triaža. Podrobnosti o razvrstitvi incidentov ne spadajo v obseg tega dokumenta. V začetku je mogoče uporabiti obrazec za razvrstitev primerov skupine CSIRT (primer za CSIRT v podjetju):

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.		

Slika 15 Shema za razvrstitev incidentov (vir: FIRST)[26]

[25] Orodja za preverjanje identitete v CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] Razvrstitev primerov skupine CSIRT http://www.first.org/resources/guides/csirt_case_classification.html

Triaža
Triaža je sistem, ki ga uporablja zdravstveno osebje ali osebje na urgenci za racionaliziranje omejenih zdravstvenih virov, kadar število poškodovanih oseb, ki so potrebne oskrbe, presega vire, ki so razpoložljivi za oskrbo, in na ta način nuditi oskrbo kar največjemu število bolnikov[27].

Skupina CERT/CC daje naslednji opis:

Triaža je osnovni element vsake dejavnosti upravljanja incidentov, predvsem za vse uveljavljene skupine CSIRT. Triaža predstavlja ključno pot pri razumevanju stvari, o katerih se poroča preko organizacije. Služi kot sredstvo, preko katerega se vse informacije stekajo v eno samo kontaktno točko, kar omogoča podjetju, da ohranja nadzor nad potekajočimi dejavnostmi in celovito vzajemnost vseh posredovanih podatkov. Triaža omogoča izvedbo začetne ocene vhodnega poročila in ga pripravi na nadaljnjo obravnavo. Prav tako predstavlja mesto za pripravo začetne dokumentacije in vnos podatkov v poročilo ali zahtevek, če ni bilo to izvedeno že v postopku odkrivanja.

Funkcije triaže dajejo takojšen posnetek trenutnega stanja vseh prijavljenih dejavnosti – katera poročila so odprta ali zaprta, katera dejanja čakajo na izvedbo in koliko poročil posamezne vrste je bilo prejetih. Ta postopek lahko pomaga pri identifikaciji potencialnih varnostnih problemov in razporeditvi delovnih procesov glede na pomembnost. S pomočjo informacij, zbranih med triažo, je mogoče pripraviti tudi smernice na področju ranljivosti in incidentov ter statistike za višje vodstvo[28].

Triaže lahko izvajajo samo najbolj izkušeni člani skupine, saj je za to potrebno dobro razumevanje morebitnih vplivov incidentov na posamezne odjemalce, prav tako pa tudi sposobnost za prejemanje odločitev, kdo izmed članov skupine je primeren za reševanje tega incidenta.

[27] Triaža na Wikipediji: http://en.wikipedia.org/wiki/Triage

[28] Določitev procesa upravljanja incidentov: http://www.cert.org/archive/pdf/04tr015.pdf

3. korak: Dejavnosti

Običajno gredo incidenti, za katere se uporabi triaža, v vrsto zahtevkov v orodju za reševanje incidentov, ki ga uporablja ena ali več oseb, ki rešujejo incidente in ki v osnovi upoštevajo te korake.

Začetna oznaka incidenta
Oznaka incidenta je lahko dodeljena že v prejšnjem koraku (na primer, ko je bil incident prijavljen prek telefona). Če ni tako, se takšna oznaka dodeli v prvem koraku in se uporablja v vseh naslednjih komunikacijah o tem incidentu.

Življenjski cikel incidenta
Reševanje incidenta ne sledi poteku korakov, ki bi na koncu pripeljali do rešitve, ampak sledi ciklu korakov, ki se ponavljajo, vse dokler ni incident končno rešen, vse vpletene stranke pa prejmejo vse potrebne informacije. Ta cikel, ki je pogostokrat poimenovan tudi „življenjski cikel incidenta“, vključuje naslednje procese:

Analiza: Analizirajo se vse podrobnosti o prijavljenem incidentu.
Pridobivanje kontaktnih informacij: Za dodatno posredovanje informacij, ki se nanašajo na incident, vsem vpletenim strankam, kot so druge skupine CSIRT, žrtvam, verjetno pa tudi lastnikom sistemov, ki so bili pri napadu zlorabljeni.
Zagotavljanje tehnične pomoči: Zagotavljanje pomoči žrtvam, da bi hitro odpravili posledice incidenta, in zbiranje dodatnih informacij o napadu.
Usklajevanje: Obveščanje ostalih vpletenih strank, kot je CSIRT, odgovorna za sistem IT, ki se je pri napadu uporabljal, ali drugih žrtev.

Ta struktura se imenuje „življenjski cikel“ zaradi tega, ker en korak vodi v drugega, zadnji korak, usklajevanje, pa lahko ponovno vodi v nove analize in cikel se ponovno začne. Ko vse vpletene stranke prejmejo in posredujejo vse potrebne informacije, se proces zaključi.

Podrobnejši opis življenjskega cikla incidenta lahko najdete v priročniku CERT/CC CSIRT[29].

Poročila o reševanju incidenta
Na vprašanja s strani vodstva o incidentu se pripravite s sestavo poročila. Prav tako je dobra praksa priprava dokumenta (namenjenega samo za notranjo uporabo) o „pridobljenih izkušnjah“, na osnovi katerega lahko osebje pridobiva izkušnje in se lahko izogne napakam v postopku reševanja incidentov v prihodnje.

Arhiviranje

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

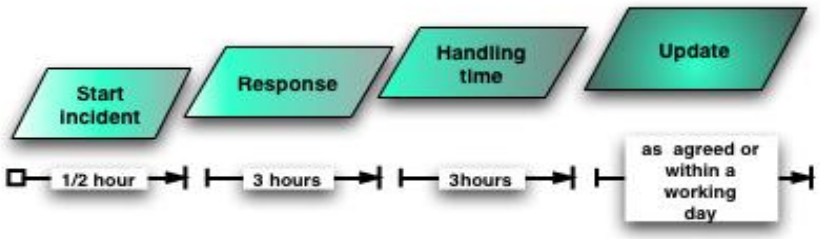
Preglejte pravila glede arhiviranja, opisana v poglavju *6.6 Priprava informacijske varnostne politike*.

Celotna navodila o upravljanju incidentov in življenjskem ciklu incidenta lahko najdete v poglavju *A.1 Dodatno gradivo* v prilogi.

8.4 Primer časovnega razporeda reševanja

Določitev odzivnih časov se pogostokrat zanemari, vendar pa mora biti del vsakega dobro sestavljenega dogovora o ravni storitev (SLA) med skupino CSIRT in njenimi odjemalci. Zagotavljanje pravočasnih povratnih informacij odjemalcem v času reševanja incidentov je ključnega pomena tako za ugled skupine kot tudi za obveznosti odjemalcev.
Da bi se bilo mogoče izogniti napačnim pričakovanjem, morajo biti odzivni časi odjemalcem jasno posredovani. Kot osnovo pri pripravi podrobnejšega dogovora SLA z odjemalci skupine CSIRT lahko uporabite naslednji osnovni časovni razpored.

Tu lahko najdete primer praktičnega časovnega razporeda odziva vse od trenutka prejema zahteve za pomoč:



Slika 16 Primer časovnega razporeda odziva

Prav tako je dobra praksa odjemalcem posredovati navodila o njihovih lastnih odzivnih časih, predvsem glede tega, kdaj se obrniti na skupino CSIRT v izrednih razmerah. V večini primerov se je bolje obrniti na skupino CSIRT že v začetni fazi, prav tako pa je dobra praksa spodbujati odjemalce, da to storijo tudi, kadar so v dvomih.

8.5 Razpoložljivo orodje skupine CSIRT

To poglavje vsebuje nekatere informacije o običajnem orodju, ki ga uporabljajo skupine CSIRT. Vsebuje samo primere, več informacij pa lahko najdete v *Center orodij za reševanje incidentov*[30] (CHIHT).

Programska oprema za šifriranje elektronske pošte in sporočil

- GNUPG http://www.gnupg.org/
  GnuPG je popolna in brezplačna izvedba standarda OpenPGP pod splošno javno licenco GNU, kot je opredeljen v dokumentu RFC2440. GnuPG omogoča šifriranje in podpisovanje podatkov in komunikacij.

- PGP http://www.pgp.com/
  Komercialna različica.

Orodje za reševanje incidentov

Upravljanje in spremljanje incidentov, evidentiranje ukrepov.

- RTIR http://www.bestpractical.com/rtir/
  RTIR je brezplačen odprto kodni sistem za reševanje incidentov, zasnovan glede na potrebe skupin CERT in drugih skupin za reševanje incidentov.

Orodja za CRM

Podatkovna baza CRM je v veliko pomoč, če imate veliko različnih odjemalcev in želite beležiti vse podrobnosti in sestanke. Obstajajo številne različice, če navedemo le nekaj primerov:

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

- Sugarforce (brezplačna odprto kodna različica) http://www.sugarforge.org/

Preverjanje informacij

- Spremljanje spletnega mesta
  http://www.aignes.com/index.htm
  Ta program spremlja spletna mesta ter išče spremembe in posodobitve.

- Watch that page http://www.watchthatpage.com/
  Storitev pošilja informacije o spremembah na spletnih mestih po elektronski pošti (brezplačna in komercialna različica).

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

Iskanje kontaktnih informacij
Iskanje ustreznega kontakta za posredovanje informacij o incidentih ni enostavno opravilo. Obstaja nekaj informacijskih virov, ki jih lahko uporabljate:

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

Tudi CHIHT navaja nekatera orodja, ki jih je mogoče uporabljati za iskanje kontaktnih informacij[34].

Navidezna CSIRT (8. korak)
Vzpostavitev procesnih tokov ter operativnih in tehničnih postopkov Navidezna skupina CSIRT je osredotočena na zagotavljanje osnovnih storitev skupine CSIRT: • Obveščanje in opozorila • Najave • Reševanje incidentov Skupina je razvila postopke, ki dobro delujejo, hkrati pa so razumljivi vsem članom skupine. Navidezna skupina CSIRT je prav tako najela pravnega strokovnjaka, ki bo deloval na področju odgovornosti in politike informacijske varnosti. Skupina uporablja nekatera uporabna orodja, prav tako pa so ji bile v pomoč informacije o operativnih vprašanjih, o katerih so razpravljali z drugimi skupinami CSIRT. Pripravljena je bila standardna predloga za svetovanje glede varnosti in poročila o incidentih. Skupina za reševanje incidentov uporablja RTIR.

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

[32] IRT-object v podatkovni bazi RIPE: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Zaupanja vredna tretja oseba: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Orodja za preverjanje identitete v CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Usposabljanje skupine CSIRT

Do sedaj smo opravili naslednje korake:

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.
2. Kateremu sektorju bo skupina CSIRT zagotavljala storitve?
3. Katere storitve lahko CSIRT zagotavlja svojim odjemalcem.
4. Analiziranje okolja in odjemalcev.
5. Določitev poslanstva.
6. Priprava poslovnega načrta.
   a. Priprava finančnega modela.
   b. Določitev organizacijske strukture.
   c. Začetek zaposlovanja osebja.
   d. Izraba in opremljanje pisarne.
   e. Razvoj politike informacijske varnosti.
   f. Iskanje partnerjev za sodelovanje.
7. Spodbujanje poslovnega načrta.
   a. Odobritev poslovnega primera.
   b. Priprava projektnega načrta.
8. Začetek delovanja skupine CSIRT.
   a. Vzpostavitev potekov dela.
   b. Uporaba orodja skupine CSIRT.

>> Naslednji korak je: Usposabljanje osebja

To poglavje navaja dva glavna vira, namenjena usposabljanju skupine CSIRT: Tečaji TRANSITS in CERT/CC.

9.1 TRANSITS

TRANSITS je bil evropski projekt z naslavljanjem težave, povezane s pomanjkanjem izkušenega osebja CSIRT, namenjen spodbujanju vzpostavljanja skupine za reševanje varnostnih incidentov (CSIRT) in izboljševanju obstoječih skupin CSIRT. Ta cilj se je začel uresničevati z zagotavljanjem specializiranih tečajev za usposabljanje osebja (novih) skupin CSIRT na področju organizacijskih, operativnih, tehničnih, tržnih in pravnih vprašanj, ki so povezani z zagotavljanjem storitev CSIRT.

TRANSITS je predvsem:

- razvil, posodobil in redno pregledoval modularno gradivo za tečaje,
- organiziral izobraževalne delavnice, kjer je bilo zagotovljeno izobraževalno gradivo,
- omogočil udeležbo osebja (novih) skupin CSIRT na teh izobraževalnih delavnicah, s poudarkom na sodelovanju skupin iz držav pristopnic EU,
- razširil izobraževalno gradivo in zagotovil uporabo rezultatov[35].

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

ENISA omogoča in podpira tečaje TRANSITS. Če vas zanima, kako se na tečaje prijaviti, ter potrebujete informacije o zahtevah in stroških, se obrnite na strokovnjaka CSIRT agencije ENISA:

CERT-Relations@enisa.europa.eu

V prilogi k temu dokumentu se nahaja vzorec izobraževalnega gradiva!

9.2 CERT/CC

Zaradi zapletenosti računalniških in omrežnih infrastruktur ter izzivov administracije je pravilno upravljanje omrežne varnosti zelo težko. Sistemski administratorji in administratorji omrežij nimajo dovolj ljudi in izkušenj na področju varnosti, da bi jih lahko ščitili pred napadi in čim bolj zmanjšali škodo. Prav zaradi tega število varnostnih incidentov vse bolj raste.
Kadar pride do računalniškega varnostnega incidenta, se morajo organizacije na to hitro in učinkovito odzvati. Hitreje ko organizacija ugotovi, analizira in se odzove na incident, lažje je mogoče omejiti škodo in zmanjšati stroške odprave. Vzpostavitev skupine za reševanje računalniških varnostnih incidentov (CSIRT) je dober način, ki omogoča hitro odzivanje, prav tako pa pomaga pri preprečevanju incidentov v prihodnje.

CERT-CC nudi tečaje za vodilne delavce in tehnično osebje na področjih, kot so vzpostavitev in vodenje skupin za reševanje računalniških varnostnih incidentov (CSIRT), odzivanje na in analiziranje varnostnih incidentov ter izboljševanje omrežne varnosti. Če ni navedeno drugače, vsi tečaji potekajo v Pittsburghu, PA. Naše osebje izvaja tečaje na področju varnosti tudi na univerzi Carnegie Mellon.

Tečaji CERT/CC[36], ki so na voljo in so namenjeni skupinam CSIRT.

Vzpostavitev skupine za reševanje varnostnih incidentov (CSIRT)
Vodenje skupin za reševanje varnostnih incidentov (CSIRT)
Osnove na področju reševanja incidentov
Napredno reševanje incidentov za tehnično osebje

V prilogi k tem dokumentom lahko najdete primer vzorca izobraževalnega gradiva!

Navidezna CSIRT (9. korak)
Usposabljanje osebja Navidezna skupina CSIRT se je odločila, da bo svoje tehnično osebje poslala na naslednje tečaje TRANSITS, ki so na voljo. Vodja skupine se bo dodatno udeležil še tečaja CERT/CC *Vodenje skupine CSIRT*.

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

10 Vaja: priprava svetovanja

Do sedaj smo opravili naslednje korake:

1. Razumevanje, kaj je CSIRT in katere prednosti lahko zagotavlja.
2. Kateremu sektorju bo skupina CSIRT zagotavljala storitve?
3. Katere storitve lahko CSIRT zagotavlja svojim odjemalcem.
4. Analiziranje okolja in odjemalcev.
5. Določitev poslanstva.
6. Priprava poslovnega načrta.
   a. Priprava finančnega modela.
   b. Določitev organizacijske strukture.
   c. Začetek zaposlovanja osebja.
   d. Izraba in opremljanje pisarne.
   e. Razvoj politike informacijske varnosti.
   f. Iskanje partnerjev za sodelovanje.
7. Spodbujanje poslovnega načrta.
   a. Odobritev poslovnega primera.
   b. Priprava projektnega načrta.
8. Začetek delovanja skupine CSIRT.
   a. Vzpostavitev potekov dela.
   b. Uporaba orodja skupine CSIRT.
9. Usposabljanje osebja.

>> Naslednji korak je vaja in priprave na dejansko delo!

To poglavje za ilustracijo opisuje enostavno vajo vsakodnevne naloge skupine CSIRT: priprava svetovanja glede varnosti.

Sprožilo jo je naslednje originalno varnostno sporočilo, ki ga je posredovalo podjetje Microsoft:

Identifikator sporočila	**Varnostno sporočilo podjetja Microsoft MS06-042**
Naslov sporočila	**Skupna varnostna posodobitev za Internet Explorer (918899)**
Povzetek za vodstvo	Ta posodobitev odpravlja številne ranljivosti programske opreme Internet Explorer, ki so omogočale oddaljeno izvajanje kode.
Največja stopnja resnosti	Kritična
Posledica ranljivosti	Oddaljeno izvajanje kode
Prizadeta programska oprema	**Windows, Internet Explorer.** Več informacij lahko najdete pod točko prizadeta programska oprema in mesta za prenos.

To sporočilo dobavitelja se nanaša na nedavno odkrito ranljivost programske opreme Internet Explorer. Dobavitelj je objavil številne popravke za to programsko opremo za številne različice operacijskega sistema Microsoft Windows.

Navidezna skupina CSIRT, po prejemu te informacije o ranljivosti prek poštnega seznama, začne z izvajanjem poteka dela, opisanega v poglavju *8.2 Priprava alarmov, opozoril in najav*.

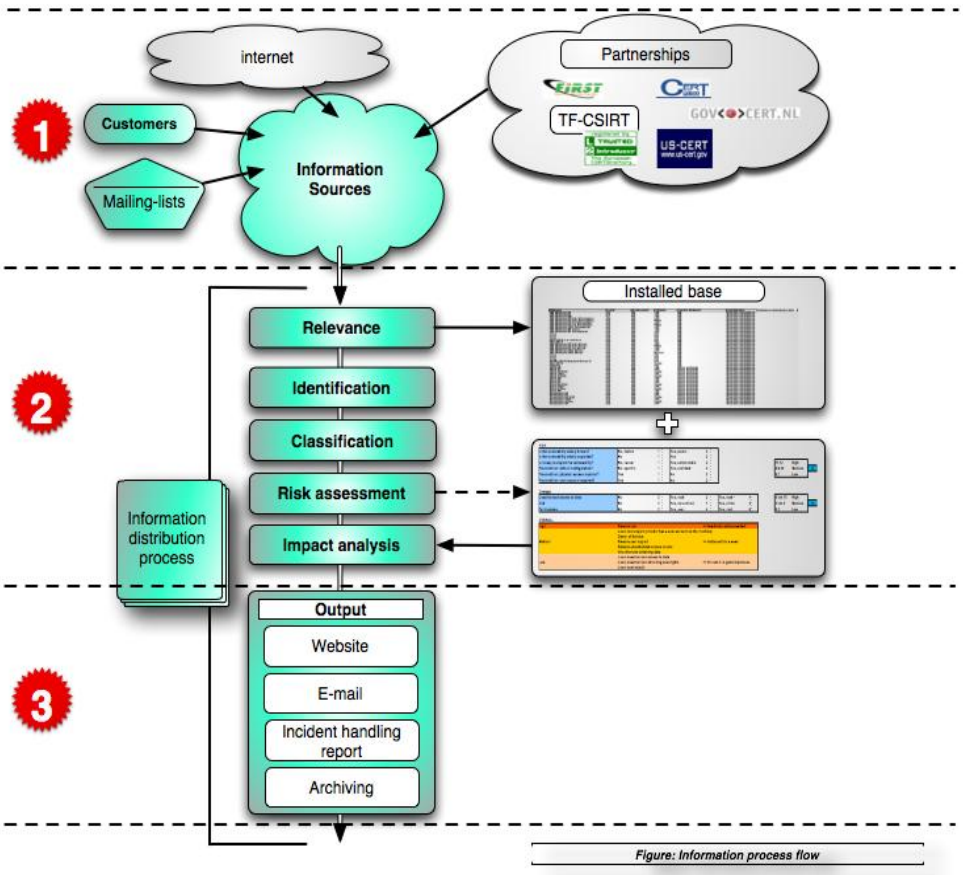


Figure: Information process flow

1. korak: Pridobivanje informacij o ranljivosti

Prvi korak je obisk spletnega mesta dobavitelja. Navidezna skupina CSIRT lahko tam preveri pristnost informacije in pridobi dodatne podrobnosti o ranljivosti in prizadetih sistemih IT.

2. korak: Presoja informacij in ocenjevanje tveganja

Identifikacija
Informacije so že bile preverjene z navzkrižnim preverjanjem informacij o ranljivosti, posredovanih po elektronski pošti, z besedilom na spletnem mestu dobavitelja.

Pomembnost
Navidezna skupina CSIRT preveri seznam prizadetih sistemov, ki ga je mogoče najti na spletnem mestu s seznamom sistemov, ki jih uporabljajo odjemalci. Skupina ugotovi, da so informacije o ranljivosti zares pomembne, saj vsaj eden izmed njenih odjemalcev uporablja Internet Explorer.

Kategorija	Aplikacija	Programska oprema proizvod	Različica	OS	OS Različica	Odjemalec
Namizje	Brskalnik	IE	x-x-	Microsoft	XP-prof	A

Klasifikacija
Informacija je javna in jo je mogoče uporabljati in posredovati.

Ocena tveganja in analize vpliva
Glede na odgovore na naslednja vprašanje je razvidno, da je tveganje in vpliv *velik* (podjetje Microsoft je tveganje označilo s stopnjo *kritično*).

TVEGANJE

Ali je ranljivost dobro poznana?	DA
Ali je ranljivost močno razširjena?	DA
Ali je ranljivost mogoče izkoristiti na enostaven način?	DA
Ali gre za ranljivost, ki jo je mogoče izkoristiti z oddaljenega mesta?	DA

ŠKODA
Možni vplivi so oddaljeno dostopanje in potencialno oddaljeno izvajanje kode. S to ranljivostjo so povezana številna vprašanja, zaradi katerih je tveganje za škodo *visoko*.

3. korak: Distribucija

Navidezna skupina CSIRT je notranja skupina CSIRT. Kot komunikacijske kanale ponuja elektronsko pošto, telefon in notranje spletno mesto. Skupina na osnovi predloge iz poglavja 8.2 *Priprava alarmov, opozoril in najav* pripravi naslednji nasvet.

Naslov nasveta
V programski opremi Internet Explorer so bile ugotovljene številne ranljivosti.

Referenčna številka
082006-1

Prizadeti sistemi
- Vsi namizni sistemi, ki uporabljajo operacijske sisteme podjetja Microsoft.

Ustrezni OS + različice
- Microsoft Windows 2000 Servisni paket 4
- Microsoft Windows XP Servisni paket 1 in Microsoft Windows XP Servisni paket 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 in Microsoft Windows Server 2003 Servisni paket 1
- Microsoft Windows Server 2003 za sisteme, ki temeljijo na Itanium platformi in Microsoft Windows Server 2003 s SP1 za sisteme, ki temeljijo na Itanium platformi
- Microsoft Windows Server 2003 x64 Edition

Tveganje (visoko-srednje-nizko)
VISOKO

Vpliv/potencialna škoda (visoka-srednja-nizka)
VISOKA

Zunanje identifikacijske številke: (identifikacijske številke običajne ranljivosti in izpostavljenosti, oglasne deske, ki vsebuje ranljivosti)
MS-06-42

Pregled ranljivosti
Podjetje Microsoft je v programski opremi Internet Explorer odkrilo številne pomanjkljivosti, ki lahko omogočijo oddaljeno izvajanje kode.

Posledice
Napadalec bi lahko prevzel popoln nadzor nad sistemom, nameščal programe, dodajal uporabnike in dostopal do, spreminjal ali brisal podatke. Olajševalni dejavnik pri tem je, da do zgoraj navedenega lahko pride samo, če je uporabnik prijavljen v sistem z administracijskimi pravicami. Negativne posledice za uporabnike, ki so v sistem prijavljeni z manjšimi pravicami, so manjše.

Rešitev
Nemudoma namestite popravke za IE.

Opis (podrobnosti)
Za več informacij si oglejte ms06-042.mspx

Priloga
Za več informacij si oglejte ms06-042.mspx

Dokument je sedaj pripravljen za distribucijo. Ker gre za kritično sporočilo, je priporočeno odjemalce poklicati, kjer je to mogoče.

Navidezna CSIRT (10. korak)
Vaja V prvih tednih delovanja je navidezna skupina CSIRT uporabila številne navidezne primere (ki so jih dobili kot primere od drugih skupin CSIRT), ki so se uporabljali pri vaji. Prav tako so izdali nekaj nasvetov glede varnosti, ki so temeljili na pravih informacijah o ranljivosti, ki so jih posredovali dobavitelji strojne in programske opreme, in jih prilagodili in uskladili s potrebami odjemalcev.

11 Zaključek

Tukaj se naš priročnik konča. Namen tega dokumenta je posredovati zelo jedrnat pregled številnih procesov, ki so potrebni za vzpostavitev skupine CSIRT. Ni popoln, prav tako pa ne vsebuje zelo podrobnih informacij. V prilogi pod točko A.1 *Dodatno gradivo* lahko najdete dodatno literaturo, ki se nanaša na to temo.

Naslednji korak za navidezno skupino CSIRT bi sedaj bil:

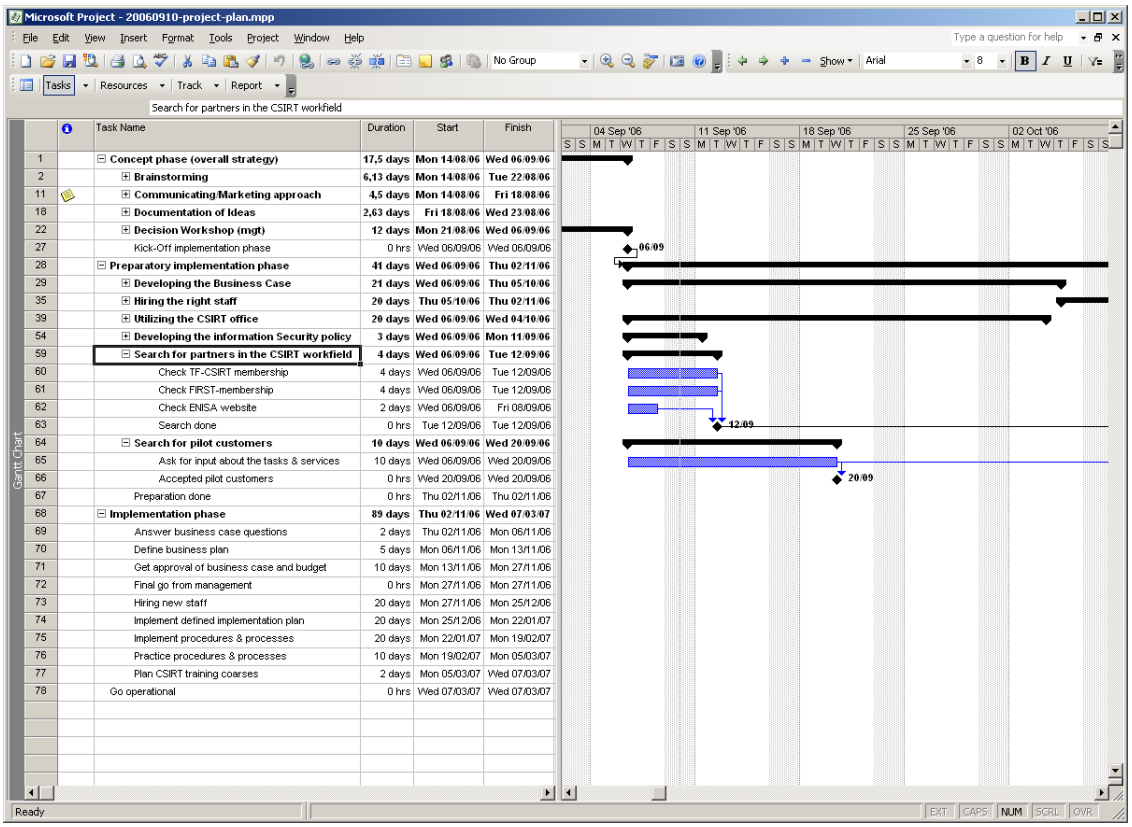
- Prejemanje povratnih informacij s strani odjemalcev, kar omogoča prilagoditev zagotovljenih storitev.
- Vzpostavitev rutinskih opravil pri vsakodnevnem delu.
- Vaja za primere izjemnih okoliščin.
- Vzdrževanje tesnih stikov s številnimi skupnostmi CSIRT z namenom vsakodnevno prispevati k njihovem delu na področju ranljivosti.

12 Opis projektnega načrta

OPOMBA: Projektni načrt daje prve ocene o potrebnem času. Dejansko trajanje projekta lahko od te ocene odstopa odvisno od razpoložljivih virov.

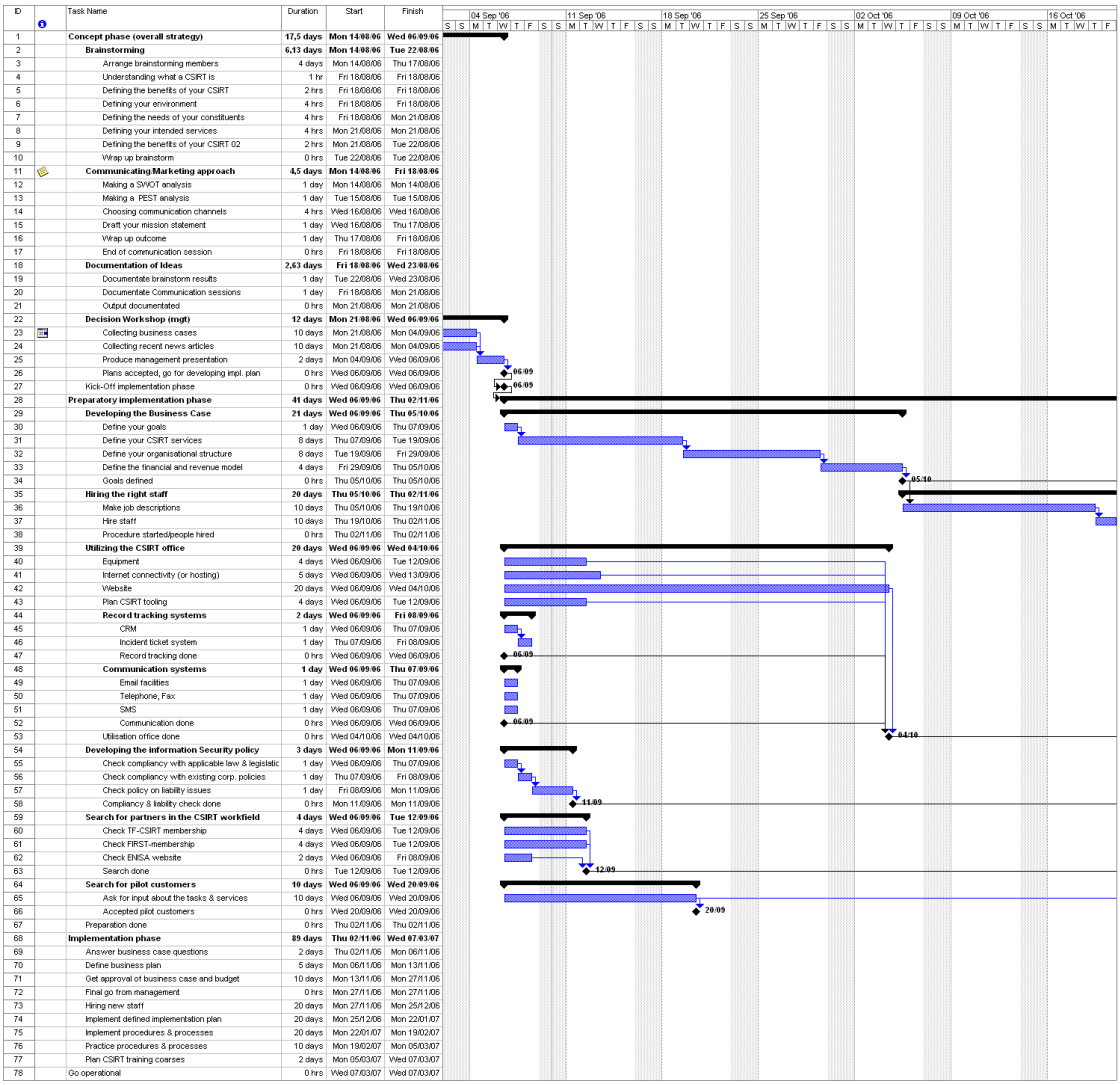
Projektni načrt je v različnih oblikah na voljo na spletih mestih ENISA in CD. V celoti pokriva vse v tem dokumentu opisane procese.

Glavna oblika dokumenta bo Microsoft Project, ki ga je mogoče neposredno uporabiti v orodju za vodenje projekta.



	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
11	Communicating/Marketing approach	4,5 days	Mon 14/08/06	Fri 18/08/06
18	Documentation of Ideas	2,63 days	Fri 18/08/06	Wed 23/08/06
22	Decision Workshop (mgt)	12 days	Mon 21/08/06	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
35	Hiring the right staff	20 days	Thu 05/10/06	Thu 02/11/06
39	Utilizing the CSIRT office	20 days	Wed 06/09/06	Wed 04/10/06
54	Developing the information Security policy	3 days	Wed 06/09/06	Mon 11/09/06
59	Search for partners in the CSIRT workfield	4 days	Wed 06/09/06	Tue 12/09/06
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	Search for pilot customers	10 days	Wed 06/09/06	Wed 20/09/06
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	Implementation phase	89 days	Thu 02/11/06	Wed 07/03/07
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Slika 17 Projektni načrt



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

Slika 18 Projektni načrt z vsemi nalogami in del grafikona Gant.

Projektni načrt je na voljo tudi v obliki CVS in XML. Dodatne oblike lahko dobite na zahtevo s strani strokovnjakov CSIRT agencije ENISA:
CERT-Relations@enisa.europa.eu

PRILOGA

A.1 Dodatno branje

Priročnik za skupine CSIRT (CERT/CC)
Zelo celovit priročnik, ki pokriva vse teme, pomembne za delo skupine CSIRT.
Vir: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Določitev procesa upravljanja incidentov za skupine CSIRT: Dokument v pripravi
Podrobne analize upravljanja incidentov
Vir: http://www.cert.org/archive/pdf/04tr015.pdf

Trenutno stanje na področju skupin za reševanje varnostnih incidentov (CSIRT)
Celovita analiza dejanskih razmer na področju skupin CSIRT po vsem svetu, vključno z zgodovino, statistiko in še veliko več.
Vir: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Celovit opis izkušenj, pridobljenih med vzpostavljanjem skupin GOVCERT.NL in 'De Waarschuwingsdienst', nizozemske nacionalne službe za obveščanje.
Vir: http://www.govcert.nl/render.html?it=69

RFC 2350: Pričakovanja na področju reševanja računalniških varnostnih incidentov.
Vir: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Priročnik za reševanje računalniških varnostnih incidentov
Vir: http://www.securityunit.com/publications/sp800-61.pdf

Seznam dejavnosti skupin CERT v Evropi agencije ENISA
Priročnik, ki vsebuje informacije o skupinah CSIRT v Evropi in njihove najrazličnejše dejavnosti.
Vir: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: Nacionalni inštitut za standarde in tehnologije

A.2 Storitve skupine CSIRT

Zahvaljujemo se CERT/CC, ki je pripravila ta seznam.

Reaktivne storitve	***Proaktivne storitve***	***Ravnanje s komponentami***
• Alarmi in opozorila • Reševanje incidentov • Analize incidentov • Reševanje incidenta na mestu samem • Podpora pri odzivanju na incidente • Usklajevanje odziva na incidente • Odpravljanje ranljivosti • Analiziranje ranljivosti • Odzivanje na ranljivosti • Usklajevanje odziva na ranljivosti	• Najave • Spremljanje tehnologije • Varnostni pregledi ali ocene • Konfiguracija in vzdrževanje varnosti • Razvoj varnostnih orodij • Storitve odkrivanja vdorov • Razširjanje informacij povezanih z varnostjo	• Analiza komponent • Odziv na komponente • Usklajevanje odziva na komponente
		Obvladovanje varnosti in kakovosti
		• Analize tveganj • Zagotavljanje neprekinjenega delovanja in ponovna vzpostavitev po nesreči • Varnostno svetovanje • Dvigovanje osveščenosti • Izobraževanje/usposabljanje • Ocenjevanje ali certificiranje produkta

Slika 19 Seznam storitev skupine CSIRT, ki ga je pripravil CERT/CC

Opis storitev

Reaktivne storitve

Reaktivne storitve so namenjene odzivanju na zahteve za pomoč, poročila o incidentih s strani odjemalcev skupine CSIRT in na vse grožnje ali napade na sisteme skupine CSIRT. Izvajanje nekaterih storitev lahko sprožijo obvestila s strani tretje stranke ali pregled spremljanja ali dnevnikov in alarmov IDS (sistem za zaznavanje vdorov).

Obveščanje in opozorila

Ta storitev obsega razširjanje informacij, ki opisujejo napad, varnostno ranljivost, alarm o vdoru, računalniških virusih ali prevarah in vsebuje vse kratkoročne priporočene ukrepe za reševanje nastale težave. Alarm, opozorilo ali nasvet se pošlje kot odziv na trenutne težave in s tem obvesti odjemalce o dejavnostih in zagotovi smernice za zaščito svojih sistemov ali obnovitev vseh sistemov, ki so bili prizadeti. Informacije lahko pripravi skupina CSIRT ali pa jih lahko posreduje naprej po tem, ko jih pridobi s strani drugih skupin CSIRT, varnostnih strokovnjakov ali drugih delov odjemalcev.

Reševanje incidentov

Reševanje incidentov obsega prejemanje, označevanje in odzivanje na zahteve in poročila, hkrati pa analizo incidentov in dogodkov. Posamezni odzivi lahko vključujejo:

- izvajanje ukrepov za zaščito sistemov in omrežij, ki so bili prizadeti ali ogroženi zaradi dejavnosti vsiljivca,
- zagotavljanje rešitev in strategij za omejevanje na osnovi ustreznih nasvetov ali alarmov,
- iskanje dejavnosti vsiljivca na drugih delih omrežja.
- filtriranje omrežnega prometa,
- ponovno vzpostavitev sistema,
- namestitev popravkov in odpravo napak na sistemih,
- pripravo drugih odzivov ali strategij, s katerimi je mogoče zaobiti težave.

Ker različne vrste skupin CSIRT izvajajo dejavnosti za reševanje incidentov na različne načine, se ta storitev na osnovi vrste izvajanih dejavnosti in vrste zagotovljene pomoči naprej deli na naslednji način:

Analiza incidentov

Obstajajo številne stopnje analize incidentov in številne podstoritve. Analiza incidentov je v bistvu pregled vseh razpoložljivih informacij in pripadajočih dokazov ali naprav, ki so povezane z incidentom ali dogodkom. Namen analize je ugotoviti obseg incidenta, obseg škode, ki je nastala zaradi incidenta, naravo incidenta in razpoložljive strategije, namenjene odzivu, ali strategije, s katerimi je mogoče zaobiti težave. Skupina CSIRT lahko rezultate, pridobljene z analizo ranljivosti in komponent (opisano spodaj), uporabi za razumevanje in zagotavljanje najpopolnejših in najbolj posodobljenih analiz, s katerimi je mogoče ugotoviti, kaj se je zgodilo na posameznem sistemu. Skupina CSIRT povezuje dejavnosti prek vseh incidentov in na ta način ugotavlja kakršne koli medsebojne povezave, smernice, vzorce ali sledi vsiljivca. Dve podstoritvi, ki se lahko glede na nalogo, cilje in procese skupine CSIRT izvajata kot del analize incidentov, sta

Forenzično zbiranje dokazov

Zbiranje, ohranjanje, dokumentiranje in analiziranje dokazov na ogroženem računalniškem sistemu za namene ugotavljanja sprememb na sistemu in lažjo rekonstrukcijo dogodkov, ki so sistem ogrozili. To zbiranje informacij in dokazov mora biti opravljeno tako, da dokumentira dokazljivo verigo lastništva, ki je sprejemljivo na sodišču v skladu s pravili dokazovanja. Naloge, ki so vključene v zbiranje dokazov, vključujejo (a niso omejene na) izvedbo kopije bitne slike trdega diska prizadetega sistema; iskanje sprememb na sistemu, kot so novi programi, datoteke, storitve in uporabniki; preverjanje delujočih procesov in odprtih vrat ter iskanje trojancev. Osebje CSIRT, ki opravlja to funkcijo, mora biti pripravljeno tudi, da lahko v sodnih postopkih sodeluje kot izvedenec.

Spremljanje ali sledenje

Sledenje izvoru vsiljivca ali identificiranje sistemov, do katerih je imel vsiljivec dostop. Ta dejavnost lahko obsega spremljanje ali sledenje, kako je vsiljivec vstopil v prizadete sisteme in povezana omrežja, katere sisteme je uporabil, da je pridobil dostop, od kje izvira napad in katere druge sisteme in omrežja je uporabil kot del napada. Prav tako lahko obsega napore za določitev identitete vsiljivca. To delo lahko skupina opravi sama, vendar običajno vključuje sodelovanje z osebjem organa pregona, ponudniki internetnih storitev ali drugimi vpletenimi organizacijami.

Reševanje incidenta na mestu samem

Skupina CSIRT zagotavlja neposredno pomoč na mestu samem, da bi s tem odjemalcem pomagala pri odpravljanju posledic incidenta. Skupina CSIRT pa ne zagotavlja le reševanja incidenta prek telefona ali elektronske pošte (glej spodaj), ampak tudi sama fizično analizira prizadete sisteme in izvede popravila in ponovno vzpostavi sistem. Te storitve obsegajo vse ukrepe na lokalni ravni, ki so potrebni, kadar obstaja sum ali dejansko pride do incidenta. Če skupina CSIRT ni na prizadetem mestu samem, njeni člani odpotujejo tja in odpravijo incident. V drugih primerih pa je lahko lokalna skupina že na mestu samem in rešuje incident kot del svojega rutinskega dela. Predvsem takrat, kadar je reševanje incidentov del običajne delovne funkcije administratorja sistema, omrežja ali administratorja za varnost, namesto vzpostavljene skupine CSIRT.

Podpora pri reševanju incidentov

Skupina CSIRT pomaga in usmerja žrtve napada pri odpravi težav zaradi incidenta prek telefona, elektronske pošte, telefaksa ali dokumentacije. To lahko vključuje tehnično pomoč pri tolmačenju zbranih podatkov, posredovanju kontaktnih informacij ali posredovanje navodil o strategijah za ponovno vzpostavitev delovanja ali omilitev posledic. Ne vključuje neposrednih ukrepov za reševanje incidentov na mestu samem, kot je opisano zgoraj. Skupina CSIRT namesto tega z oddaljenega mesta usmerja osebje, da lahko le-to samo odpravi težave.

Usklajevanje odziva na incidente

Skupina CSIRT usklajuje reševanje med strankami, ki jih je incident prizadel. To običajno vključuje žrtev napada, druge strani, vključene v napadu, in vse strani, ki potrebujejo pomoč pri analiziranju napada. Vključene so lahko tudi stranke, ki žrtvam zagotavljajo podporo IT, kot so ponudniki internetnih storitev, druge skupine CSIRT ter sistemski administratorji in administratorji omrežja na mestu samem. Usklajevanje lahko vključuje zbiranje kontaktnih informacij, obveščanje strani o njihovi morebitni vpletenosti (kot žrtve ali viri napada), zbiranje statističnih podatkov o številu vpletenih strani ter omogočanje lažje izmenjave informacij in analiz. Del usklajevanja lahko vključuje tudi obveščanje in sodelovanje s pravnim oddelkom, kadrovskim oddelkom in oddelkom za stike z javnostmi organizacije. Prav tako vključuje usklajevanje z zakonodajnim organom. Ta storitev ne vključuje neposrednih ukrepov za reševanje incidentov na mestu samem.

Odpravljanje ranljivosti

Odpravljanje ranljivosti vključuje sprejemanje informacij in poročil o ranljivostih programske in strojne opreme; analiziranje narave, delovanja in vplivov ranljivosti; in razvoj strategij odzivanja za namene odkrivanja in odpravljanja ranljivosti. Ker različne vrste skupin CSIRT izvajajo dejavnosti za odpravo ranljivosti na različne načine, je ta storitev na osnovi vrste izvajanih dejavnosti in na osnovi vrste zagotovljene pomoči nadalje razdeljena na naslednji način:

Analiza ranljivosti

Skupina CSIRT izvaja tehnične analize in preglede ranljivosti strojne in programske opreme. To vključuje tudi preverjanje domnevnih ranljivosti in tehnične preglede na

področju ranljivosti strojne in programske opreme, z namenom ugotavljanja, kje ta ranljivost je in kako jo je mogoče zlorabiti. Analiza lahko vključuje spreminjanje izvorne kode, uporabo razhroščevalnika za ugotavljanje, kje nastopi ranljivost, ali poskušanje reprodukcije problema na testnem sistemu.

Odziv v primeru ranljivosti

Ta storitev vključuje določevanje ustreznega odziva za namen omejevanja ali odprave ranljivosti. To lahko vključuje tudi razvoj ali raziskavo popravkov in rešitev, s katerimi je mogoče zaobiti težave. Prav tako vključuje obveščanje drugih o strategiji za omejevanje, če je le mogoče s pripravo in distribucijo nasvetov ali alarmov. Ta storitev lahko vključuje izvajanje odziva z nameščanjem popravkov ali rešitev, s katerimi je mogoče zaobiti težave.

Usklajevanje odziva v primeru ranljivosti

Skupina CSIRT obvešča številne dele podjetja ali odjemalce o ranljivosti in izmenjuje informacije o tem, kako zmanjšati ranljivost. Skupina CSIRT preverja, ali je bila strategija odzivanja na ranljivost uspešno izvedena. Ta storitev lahko vključuje komunikacijo z dobavitelji, drugimi skupinami CSIRT, tehničnimi strokovnjaki, člani odjemalcev in posamezniki ali skupinami, ki so prve našle ali prijavile ranljivost. Dejavnosti vključujejo izvajanje analiz ranljivosti ali poročila o ranljivosti; usklajevanje časovnega razporeda izdaje ustreznih dokumentov, popravkov ali rešitev, s katerimi je mogoče zaobiti težave; in sintetiziranje tehničnih analiz, ki so jih opravile različne stranke. Ta storitev lahko prav tako vključuje vzdrževanje javnega ali zasebnega arhiva ali baze s podatki o ranljivostih in ustreznih strategijah odziva.

Ravnanje s komponentami

Komponenta je vsaka datoteka ali objekt na sistemu, ki lahko sodeluje pri iskanju ranljivosti ali napadu na sisteme in omrežja ali ki se uporablja za odpravljanje varnostnih ukrepov. Komponente lahko vključujejo, a niso omejene na, računalniške viruse, trojanske programe, črve, zlonamerne skripte in pripomočke.
Odstranjevanje komponent vključuje pridobivanje kopij in informacij o komponentah, ki se uporabljajo pri vsiljivih napadih, izvidovanje in druge nedovoljene ali škodljive dejavnosti. Po prejemu se opravi pregled komponente. To vključuje analiziranje narave, delovanja, različice in uporabe komponente; in razvijanje (ali priporočanje) strategij za odzivanje, namenjenih odkrivanju, odstranjevanju in zaščiti pred temi komponentami. Ker različne vrste skupin CSIRT izvajajo dejavnosti za odstranjevanje komponent na različne načine, se ta storitev na osnovi vrste izvajanih dejavnosti in vrste zagotovljene pomoči naprej deli na naslednji način:

Analiza komponent

Skupina opravlja tehnične preglede in analizira vse ugotovljene komponente, ki so na sistemu. Opravljena analiza lahko vključujejo identificiranje vrste datotek in strukture komponent, primerjanje novih komponent z obstoječimi komponentami ali drugimi različicami iste komponente z namenom iskanja razlik, obratnega inženiringa ali razgrajevanje kode z namenom ugotavljanja namena in funkcije komponente.

Odziv na komponente

Ta storitev vključuje določevanje ustreznih ukrepov za zaznavanje in odstranjevanje komponent s sistema, prav tako pa ukrepe za preprečevanje nameščanja komponent. Ti so na primer ustvarjanje podpisov, ki jih je možno dodati k protivirusni programski opremi ali sistemu za zaznavanje vdorov.

Usklajevanje odziva na komponente

Ta storitev vključuje izmenjavo in sintetiziranje rezultatov analiz in strategij za odzivanje, ki se nanašajo na komponento, z drugimi raziskovalci, skupinami CSIRT, dobavitelji in drugimi varnostnimi strokovnjaki. Dejavnosti vključujejo obveščanje drugih in sintetiziranje tehničnih analiz, pridobljenih iz različnih virov. Dejavnosti lahko vključujejo tudi vzdrževanje javnega arhiva ali arhiva za stranke o vseh poznanih komponentah, njihovih vplivih in ustreznih strategijah za odzivanje.

Proaktivne storitve

Proaktivne storitve so namenjene izboljševanju odjemalčeve infrastrukture in varnostnih procesov še preden se zgodi ali je zaznan kakršen koli incident ali dogodek. Glavni nameni pri tem je izogniti se incidentom in zmanjšati njihov vpliv in obseg, kadar do njih pride.

Najave

Te vključujejo, a niso omejene na, alarme glede vdorov, opozorila glede ranljivosti in nasvete glede varnosti. S takšnimi najavami je mogoče odjemalce obveščati o novostih na področju srednje- in dolgoročnih vplivov, kot so na novo ugotovljene ranljivosti ali orodja vsiljivcev. Najave omogočajo odjemalcem, da ščitijo svoje sisteme in omrežja pred novo odkritimi težavami, še preden jih je mogoče zlorabiti.

Spremljanje tehnologije

Skupina CSIRT spremlja in nadzira novosti na področju tehničnega razvoja, dejavnosti vsiljivcev in povezane smernice, kar pomaga pri prepoznavanju groženj v prihodnosti. Teme, ki jih skupina spremlja, je mogoče tudi razširiti, tako da vključujejo pravne in zakonodajne odločitve, socialne ali politične grožnje in pojavljajoče tehnologije. Ta storitev vključuje spremljanje poštnih seznamov in spletnih mest, ki se nanašajo na varnost, ter trenutnih novic in člankov v revijah na področju znanosti, tehnologije, politike in vlade, da bi na ta način bilo mogoče pridobiti informacije, ki so pomembne za varnost sistemov in omrežij odjemalcev. To lahko vključuje komunikacijo z drugimi stranmi, ki so glavne na tem področju, da se na ta način zagotovi pridobivanje najboljših in najbolj natančnih razlag. Rezultat te storitve je lahko neka vrsta najave, smernic ali priporočil, ki so osredotočene na bolj srednje- in dolgoročna varnostna vprašanja.

Varnostni pregledi ali ocene

Ta storitev daje podroben pregled in analize varnostne infrastrukture v organizaciji, in sicer na osnovi zahtev, ki jih je podala organizacija, ali drugih industrijskih standardov, ki veljajo. Obsega lahko tudi pregled varnostnih praks v organizaciji. Obstajajo številne vrste pregledov ali ocen, ki jih je mogoče zagotavljati, in sicer

Pregled infrastrukture

Ročno pregledovanje konfiguracije strojne in programske opreme, usmerjevalnikov, požarnih zidov, strežnikov in namiznih naprav, da bi bilo mogoče zagotoviti, da ustrezajo organizacijskim ali industrijskim najboljšim varnostnim politikam in standardnim konfiguracijam.

Pregled najboljših praks

Opravljanje razgovorov z zaposlenimi in administratorji sistemov in omrežij, da bi bilo mogoče ugotoviti, ali njihove varnostne politike ustrezajo izbrani organizacijski varnostni politiki ali drugim posebnim industrijskim standardom.

Skeniranje

Uporaba programske opreme za iskanje ranljivosti ali virusov, s pomočjo katere je mogoče ugotoviti, kateri sistemi in omrežja so ranljivi.

Penetracijski test

Testiranje varnosti mesta z namernim napadanjem njegovih sistemov in omrežij.
Pred izvajanjem takšnih pregledov ali ocen je potrebno pridobiti dovoljenje višjega vodstva. Politika organizacije lahko izvajanje nekaterih izmed teh pristopov prepoveduje. Del zagotavljanja te storitve je lahko tudi razvoj skupnega nabora praks, na katerih se izvedejo testi ali ocene, skupaj z razvojem zahtevanih zahtev glede certifikacije ali usposobljenosti osebja, ki izvaja testiranje, ocenjevanje, preglede ali revizije. Te storitve lahko opravlja tudi tretja stranka pogodbenica ali ponudnik storitev obvladovanja varnosti z ustreznimi strokovnimi znanji na področju opravljanja pregledov in ocen.

Postavitev in vzdrževanje varnostni orodij, aplikacij, infrastrukture in storitev

Ta storitev pomaga pri identificiranju ali zagotavljanju ustreznih smernic o tem, kako varno nastaviti in vzdrževati orodja, aplikacije ter osnovno računalniško infrastrukturo, ki jo uporabljajo odjemalci ali skupina CSIRT. Skupina CSIRT lahko poleg priprave smernic izvede tudi posodobitve konfiguracije in vzdrževanje varnostnih orodij in storitev, kot so IDS, sistemi za skeniranje ali spremljanje omrežij, filtri, ovojnice, požarni zidovi, navidezna zasebna omrežja (VPN) ali mehanizmi za preverjanje istovetnosti. Skupina CSIRT lahko te storitve zagotavlja tudi kot del glavne funkcije. Skupina CSIRT lahko skrbi tudi za konfiguriranje in vzdrževanje strežnikov, namiznih in prenosnih računalnikov, osebnih digitalnih pripomočkov (PDA) in drugih brezžičnih naprav v skladu z varnostnimi usmeritvami. Ta storitev vključuje tudi obveščanje vodstva o vseh vprašanjih in težavah s konfiguracijami ali uporabo orodij in aplikacij, za katere skupina CSIRT meni, da lahko povzročijo ranljivost na sistemih.

Razvoj varnostnih orodij

Ta storitev vključuje razvoj vseh novih orodij, prilagojenih potrebam odjemalcev, ki jih zahtevajo ali si jih željo odjemalci sami ali pa skupina CSIRT. To lahko na primer vključuje razvoj varnostnih popravkov za prilagojeno programsko opremo, ki jo uporablja odjemalec, ali zaščitenih programskih distribucij, ki se lahko uporabljajo za ponovno vzpostavitev prizadetih gostiteljev. Vključuje lahko tudi razvojna orodja ali skripte, ki razširijo funkcionalnost obstoječih varnostnih orodij, kot so novi vtičniki za programe, namenjene iskanju ranljivosti ali skeniranju omrežij, skripte, ki olajšajo tehnologijo za šifriranje, ali mehanizmi za avtomatsko distribucijo popravkov.

Storitve zaznavanja vdorov

Skupine CSIRT, ki zagotavljajo to storitev, preverjajo obstoječe dnevnike IDS, analizirajo in pripravljajo odzive na vse dogodke, ki ustrezajo določenim pogojem, ali posredujejo vse alarme v skladu s predhodno določenim dogovorom o ravni storitev ali eskalacijski strategiji. Zaznavanje vdorov in analiziranje ustreznih varnostnih dnevnikov je lahko zahtevno opravilo – ne samo zaradi tega, ker je treba ugotoviti, kam v okolju postaviti senzorje, ampak tudi zaradi zbiranja in analiziranja velike količine zbranih podatkov. V številnih primerih je za sintetiziranje in razlago informacij potrebno posebno orodje ali znanje, kar omogoča prepoznavanje napačnih alarmov, napak ali omrežnih dogodkov in izvajanje strategij, namenjenih za odpravo ali čim večje zmanjšanje takšnih dogodkov. Nekatere organizacije se odločijo, da bodo za izvajanje teh dejavnosti najele druge osebe, ki imajo več strokovnega znanja pri zagotavljanju teh storitev, kot so ponudniki storitev obvladovanja varnosti.

Razširjanje informacij, ki se nanašajo na varnost

Ta storitev ponuja odjemalcem celovito in za uporabo enostavno zbirko uporabnih informacij, ki pomaga pri izboljševanju varnosti. Takšne informacije lahko vključujejo:

- smernice glede poročanja in kontaktne informacije skupine CSIRT;
- arhive z alarmi, opozorili in drugimi najavami;
- dokumentacijo o trenutnih najboljših praksah;
- splošne smernice glede računalniške varnosti;
- politike, postopke in kontrolne sezname;
- informacije o popravkih in distribuciji;
- povezave do dobaviteljev;
- trenutne statistične informacije in smernice na področju poročanja o incidentih;
- druge informacije, ki lahko celostno izboljšajo varnostne politike.

Te informacije lahko pripravi in objavi skupina CSIRT ali drug del organizacije (IT, kadrovska služba ali služba za odnose z mediji) in lahko vključujejo informacije, navedene v zunanjih virih, kot so druge skupine CSIRT, dobavitelji in varnostni strokovnjaki.

Storitve obvladovanja kakovosti

Storitve, ki spadajo v to kategorijo, niso omejene samo na reševanje incidentov ali posebej na skupino CSIRT. So dobro poznane, uveljavljene storitve, namenjene izboljšanju celotne varnosti organizacije. Skupina CSIRT lahko z uporabo izkušenj, pridobljenih pri zagotavljanju zgoraj opisanih reaktivnih in proaktivnih storitev, vzpostavi edinstvene vidike k tem storitvam obvladovanja, ki drugače ne bi bile na voljo. Te storitve so oblikovane tako, da vključujejo povratne informacije in znanja, pridobljena s pomočjo odzivanja na incidente, ranljivosti in napade. Posredovanje takšnih izkušenj v uveljavljene običajne storitve (opisane zgoraj) kot del procesa obvladovanja kakovosti na področju varnosti lahko izboljša dolgoročna prizadevanja na področju varnosti v organizaciji. Skupina CSIRT lahko v odvisnosti od organizacijske strukture in odgovornosti te storitve zagotavlja ali sodeluje pri njih kot del prizadevanj skupine v večji organizaciji.
Naslednji opisi vsebujejo razlage, kako lahko strokovno znanje skupine CSIRT prinese koristi za vsako takšno storitev vodenja kakovosti na področju varnosti.

Analiza tveganja

Skupine CSIRT lahko doprinesejo k boljšim analizam tveganja in ocenam. To lahko izboljša sposobnost organizacije, da oceni dejanska tveganja, izvede realne kvalitativne in kvantitativne ocene tveganj za informacijska sredstva ter ovrednoti strategije odziva in zaščite. Skupine CSIRT, ki zagotavljajo to storitev, izvajajo ali pomagajo pri izvajanju analiz za ugotavljanje tveganja na področju informacijske varnosti pri novih sistemih in poslovnih procesih ali pri ocenjevanju groženj in napadov na sredstva in sisteme odjemalcev.

Neprekinjeno poslovanje in načrtovanje obnovitve po nesreči

Vse več incidentov lahko ima na osnovi preteklih pojavov in napovedi za prihodnost na področju pojava incidentov ali varnostnih smernic za posledico resno ohromitev poslovanja. Zaradi tega je pri načrtovanju najboljšega odziva na takšne incidente treba upoštevati izkušnje in priporočila skupine CSIRT, da bi bilo mogoče s tem zagotoviti neprekinjeno poslovanje. Skupine CSIRT, ki zagotavljajo to storitev, sodelujejo pri načrtovanju neprekinjenega poslovanja in obnovitve po nesreči za dogodke, povezane s tveganji za varnost računalnikov in napadi.

Svetovanje na področju varnosti

Skupine CSIRT lahko sodelujejo pri usmerjanju in svetovanju glede najboljših varnostnih praks, ki jih je treba izvesti glede na poslovanje odjemalca. Skupina, ki opravlja to storitev, sodeluje pri pripravi priporočil ali določevanju zahtev glede nakupa, namestitve in zaščite novih sistemov, omrežnih naprav, programskih aplikacij ali poslovnih procesov, ki potekajo na ravni podjetja. Ta storitev vključuje zagotavljanje smernic in pomoči pri razvoju varnostnih politik za organizacijo ali odjemalca. Vključuje lahko tudi zagotavljanje pričanj ali svetovanja zakonodajnim ali drugim vladnim organom.

Dviganje osveščenosti

Skupine CSIRT lahko ugotovijo, na katerih področjih odjemalci potrebujejo več informacij, in jih pri tem usmerjajo k vzpostavljanju boljše skladnosti s sprejetimi varnostnimi politikami in varnostnimi politikami organizacije. Povečevanje splošne osveščenosti glede varnosti pri odjemalcih ne izboljša le njihovega razumevanja varnostnih vprašanj, ampak jim prav tako pomaga pri opravljanju vsakodnevnih opravil na varnejši način. To lahko zmanjša pojavnost uspešnih napadov in poveča verjetnost, da bodo odjemalci zaznali in prijavili napade ter s tem zmanjšali čas, potreben za ponovno vzpostavitev, in odpravili ali zmanjšali izgube.
Skupine CSIRT, ki zagotavljajo to storitev, poskušajo dvigniti osveščenost glede varnosti s pripravo člankov, letakov, časopisov, spletnih mest ali drugih informativnih virov, ki razlagajo najboljše prakse na področju varnosti in svetujejo glede ukrepov, ki jih je treba izvajati. Dejavnosti lahko vključujejo tudi načrtovanje sestankov in seminarjev, na katerih se lahko odjemalci seznanijo z najnovejšimi spoznanji na področju varnostnih postopkov in potencialnih groženj za sisteme v organizaciji.

Izobraževanje/usposabljanje

Ta storitev vključuje posredovanje informacij odjemalcem o vprašanjih glede računalniške varnosti s seminarji, delavnicami, tečaji in vajami. Teme se lahko nanašajo na smernice glede prijave incidentov, ustrezne metode odzivanja, orodja za reševanje

incidentov, metode za preprečevanje incidentov in druge informacije, potrebne za zaščito, ugotavljanje, poročanje in odzivanje na incidente, povezane z računalniško varnostjo.

Ocenjevanje in certificiranje produkta

Pri tej storitvi lahko skupina CSIRT opravi ocenjevanje orodij, aplikacij ali drugih storitev, da bi bila s tem zagotovljena varnost produktov in njihova skladnost z veljavnimi varnostnimi praksami skupine CSIT ali organizacije. Pregledana orodja in aplikacije so lahko komercialni ali odprto kodni produkti. To storitev je mogoče zagotavljati kot ocenjevanje ali s certifikacijskim programom, glede na standarde, ki jih je uvedla organizacija ali skupina CSIRT.

A.3 Primeri

Navidezna skupina CSIRT

0. korak – Razumevanje, kaj je skupina CSIRT:

Vzorčna CSIRT bo služila potrebam srednje velike ustanove, ki jo sestavlja 200 članov osebja. Ustanova ima svoj oddelek IT in še dve drugi poslovalnici v isti državi. IT v podjetju igra ključno vlogo, saj se uporablja za notranjo komunikacijo, podatkovno omrežje in e-poslovanje 24 ur na dan, 7 dni v tednu. Ustanova ima svoje omrežje in razpolaga z redundančno povezavo do interneta prek dveh različnih ponudnikov internetnih storitev.

- -

1. korak: Začetna faza

V začetni fazi se nova skupina CSIRT načrtuje kot notranja skupina CSIRT, ki zagotavlja svoje storitve družbi gostiteljici, lokalnemu oddelku IT in osebju. Prav tako nudi podporo in usklajuje reševanje varnostnih incidentov, povezanih z IT, med različnimi podružnicami.

- -

2. korak: Izbira pravih storitev

V začetni fazi je sprejeta odločitev, da bo CSIRT osredotočena predvsem na zagotavljanje nekaterih osnovnih storitev zaposlenim.

Po poskusni fazi se sprejme odločitev o razširitvi nabora storitev, doda pa se lahko tudi storitev obvladovanja varnosti. Ta odločitev bo sprejeta na osnovi povratnih informacij poskusnih odjemalcev in v tesnem sodelovanju z oddelkom za zagotavljanje kakovosti.

- -

3. korak: Izvajanje analiz odjemalcev in ustrezni komunikacijski kanali

Na sestanku viharjenja možganov z nekaj ključnimi vodilnimi osebami in odjemalci je bilo zbranih dovolj vhodnih informacij za izvedbo analiz SWOT. Posledica tega je ugotovitev, da obstaja potreba po ključnih storitvah:

- obveščanje in opozorila,
- reševanje incidentov (analiza, podpora pri pripravi odziva in usklajevanje odzivov),
- najave.

Treba je zagotoviti, da se informacije posredujejo na dobro organiziran način, ki zajema največje možno število odjemalcev. Sprejeta je odločitev, da bodo alarmi, opozorila in najave v obliki nasvetov glede varnosti objavljeni na namenskem spletnem mestu in razposlani prek seznama poštnih naslovov. Za prejemanje poročil o incidentih skupina CSIRT uporablja e-pošto, telefon in telefaks. Kot naslednji korak se načrtuje priprava poenotenega spletnega obrazca.

4. korak: Poslanstvo

Vodstvo navidezne skupine CSIRT je pripravilo naslednjo izjavo o poslanstvu:
„Navidezna skupina CSIRT nudi osebju svojih gostujočih podjetij informacije in pomoč pri zmanjševanju tveganj za računalniške varnostne incidente, prav tako pa se odziva na takšne incidente, kadar do njih pride.“

S tem navidezna skupina CSIRT jasno opredeljuje, da je notranja skupina CSIRT in da je njena glavna dejavnost reševanje vprašanj, povezanih z informacijsko tehnologijo.

- -

5. korak: Priprava poslovnega načrta

Finančni model
Na osnovi dejstva, da ima podjetje vzpostavljeno e-poslovanje 24 ur na dan, 7 dni v tednu, prav tako pa tudi oddelek IT, ki deluje 24 ur na dan, 7 dni v tednu, je sprejeta odločitev, da bo zagotavljalo vse storitve v uradnem času, izven uradnih ur pa delo na poziv. Odjemalcem bodo storitve na voljo brezplačno, v fazi priprave in ocenjevanja pa se bo preučila možnost zagotavljanja storitev zunanjim strankam.

Model prihodkov
Skupina CSIRT se bo v začetni in poskusni fazi financirala prek podjetja gostitelja. V poskusni fazi in fazi ocenjevanja bodo proučeni tudi dodatni viri financiranja, vključno z možnostjo prodaje storitev zunanjim strankam.

Organizacijski model
Ker je organizacija gostiteljica majhno podjetje, je bil izbran model vgraditve.
V uradnih urah bodo osnovne storitve (distribucija varnostnih nasvetov in reševanje/usklajevanje incidentov) zagotavljale tri osebe.

V oddelku IT so že zaposlene osebe z ustreznimi izkušnjami. S tem oddelkom se sklene sporazum, tako da lahko nova skupina CSIRT po potrebi zahteva podporo za posamezne projekte. Prav tako lahko uporablja drugo linijo tehnikov na poziv.
Osnovna skupina CSIRT bo sestavljena iz štirih članov s polnim delovnim časom in petih dodatnih članov skupine CSIRT. Eden izmed teh prav tako sodeluje v izmenah.

Osebje
Vodja skupine CSIRT ima izkušnje na področju varnosti in podpore na prvi in drugi stopnji, prav tako pa je opravljal delo na področju kriznega upravljanja. Ostali trije člani skupine so strokovnjaki za varnost. Člani skupine CSIRT, ki niso zaposleni za poln delovni čas in so iz oddelka IT, so strokovnjaki na področju infrastrukture podjetja.

5. korak: Uporaba poslovnih prostorov in politike informacijske varnosti
Oprema prostorov in njihova lokacija
Ker ima podjetje gostitelj že vzpostavljeno učinkovito fizično varnost, je nova skupina CSIRT s tega vidika dobro pokrita. V primeru izjemnih razmer je zagotovljena „vojna soba", ki omogoča usklajevanje. Za občutljivo dokumentacijo in šifrirano gradivo se zagotovi sef. Vzpostavljena je bila ločena telefonska linija, vključno s telefonsko centralo, kar omogoča delovanje klicnega centra v uradnih urah in službenega mobilnega telefona „na poziv" za čas izven uradnih ur z isto telefonsko številko.

Za objavo informacij, povezanih s skupino CSIRT, je mogoče uporabiti tudi obstoječo opremo in spletno stran podjetja. Vzpostavljena in vzdrževana je programska oprema za poštne sezname z omejenim delom za komunikacijo med člani skupine in drugimi skupinami. Vse kontaktne informacije o osebju so shranjene v podatkovni bazi, izpis teh podatkov pa se hrani v sefu.

Ureditev
Ker je bila skupina CSIRT vzpostavljena znotraj podjetja z obstoječimi politikami varnosti informacij, so bile ustrezne politike za skupino CSIRT pripravljene s pomočjo pravnega svetovalca podjetja.
- -
7. korak: Iskanje sodelovanja
S pomočjo seznama agencije ENISA je bilo mogoče hitro najti nekaj skupin CSIRT v isti državi in z njimi tudi navezati stike. Za novega voditelja skupine je bil organiziran obisk ene izmed teh skupin. Seznanil se je z državnimi dejavnostmi skupine CSIRT in se udeležil sestanka.
Ta sestanek je bil več kot koristen pri zbiranju primerov delovnih metod in pridobivanju podpore s strani drugih dveh skupin.- -
8. korak: Spodbujanje poslovnega načrta

Sprejeta je odločitev o zbiranju podatkov iz zgodovine podjetja. S tem bo možen statistični pregled nad razmerami na področju varnosti IT. To zbiranje se bo nadaljevalo tudi po začetku delovanja skupine CSIRT, da bi na ta način statistični podatki ostali posodobljeni.

Opravljeno je bilo tudi posvetovanje z drugimi nacionalnimi skupinami CSIRT o njihovih poslovnih primerih. Te skupine so pripravile nekaj diapozitivov z informacijami o nedavnih dogodkih, povezanih z incidenti na področju varnosti IT, in o stroških, ki so jih povzročili ti incidenti.

V tem primeru navidezne skupine CSIRT vodstva ni bilo potrebno prepričevati o pomembnosti poslovnih procesov IT in prav zaradi tega ni bilo težko pridobiti dovoljenja za izvedbo prvega koraka. Pripravljena sta bila poslovni primer in projektni načrt, vključno z oceno stroškov vzpostavitve in stroškov, povezanih z delovanjem.
- -

9. korak: Vzpostavitev procesnih tokov ter operativnih in tehničnih postopkov
Navidezna skupina CSIRT je osredotočena na zagotavljanje osnovnih storitev skupine CSIRT:

- Obveščanje in opozorila
- Najave
- Reševanje incidentov

Skupina je razvila postopke, ki dobro delujejo, hkrati pa so razumljivi vsem članom skupine. Navidezna skupina CSIRT je prav tako najela pravnega strokovnjaka, ki bo deloval na področju odgovornosti in politike informacijske varnosti. Skupina uporablja nekatera uporabna orodja, prav tako pa so ji bile v pomoč informacije o operativnih vprašanjih, o katerih so razpravljali z drugimi skupinami CSIRT.

Pripravljena je bila standardna predloga za svetovanje glede varnosti in poročila o incidentih. Skupina za reševanje incidentov uporablja RTIR.

- -

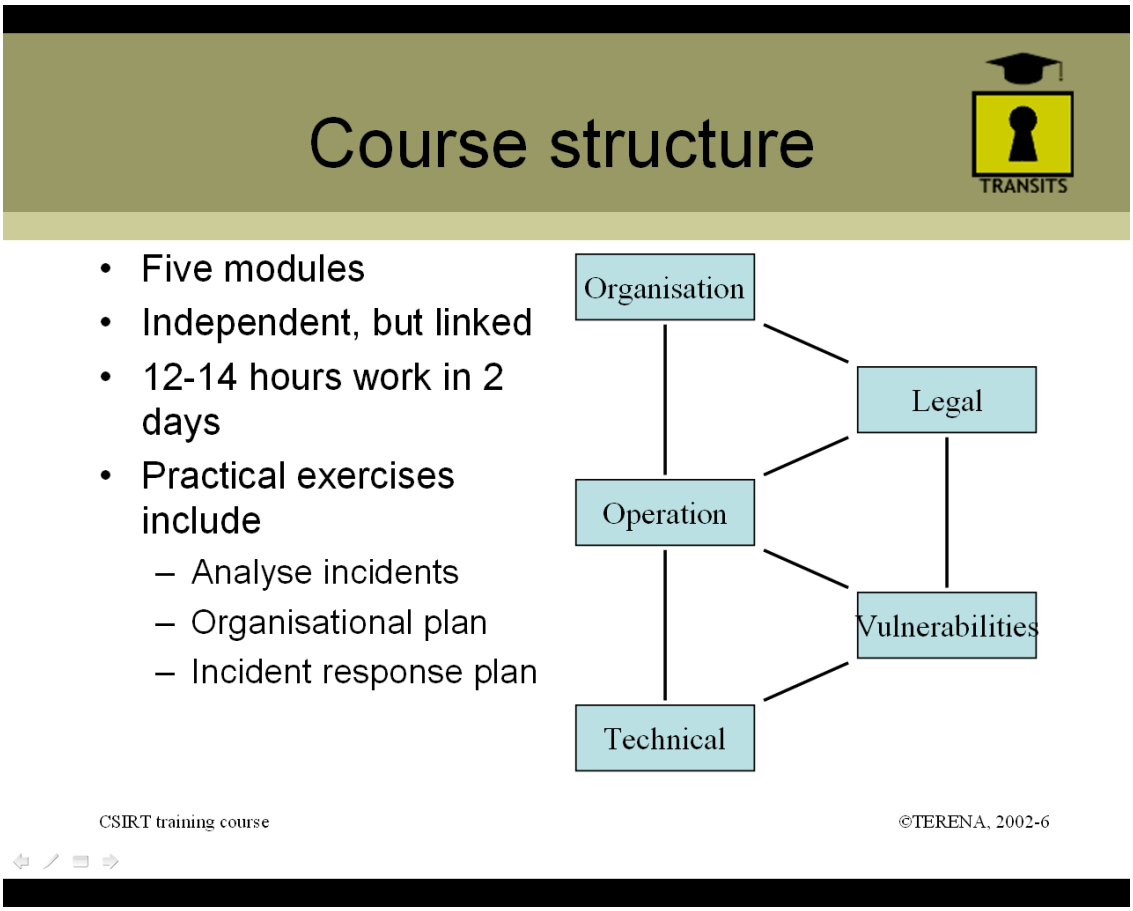
10. korak Usposabljanje osebja
Navidezna skupina CSIRT se je odločila, da bo svoje tehnično osebje poslala na naslednje tečaje TRANSITS, ki so na voljo. Vodja skupine se bo dodatno udeležil še tečaja CERT/CC *Vodenje skupine CSIRT*.

- -

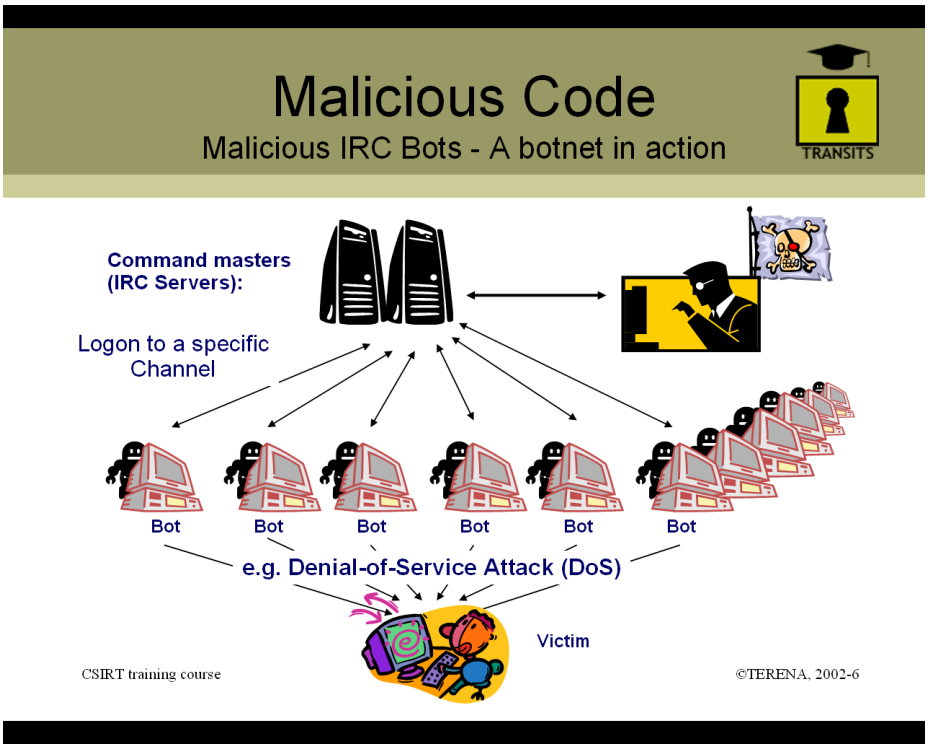
11. korak: Vaja
V prvih tednih delovanja je navidezna skupina CSIRT uporabila številne navidezne primere (ki so jih dobili kot primere od drugih skupin CSIRT), ki so se uporabljali pri vaji. Prav tako so izdali nekaj nasvetov glede varnosti, ki so temeljili na pravih informacijah o ranljivosti, ki so jih posredovali dobavitelji strojne in programske opreme, in jih prilagodili in uskladili s potrebami odjemalcev.

A.4 Vzorčno gradivo s tečajev skupine CSIRT

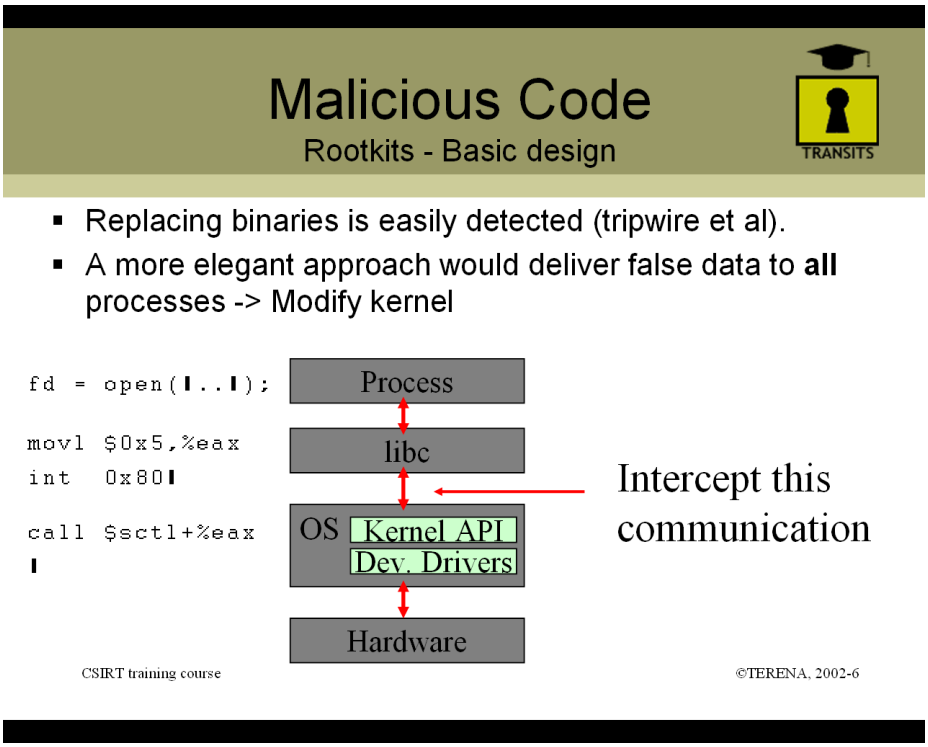
TRANSITS (s privoljenjem Terena, http://www.terena.nl)



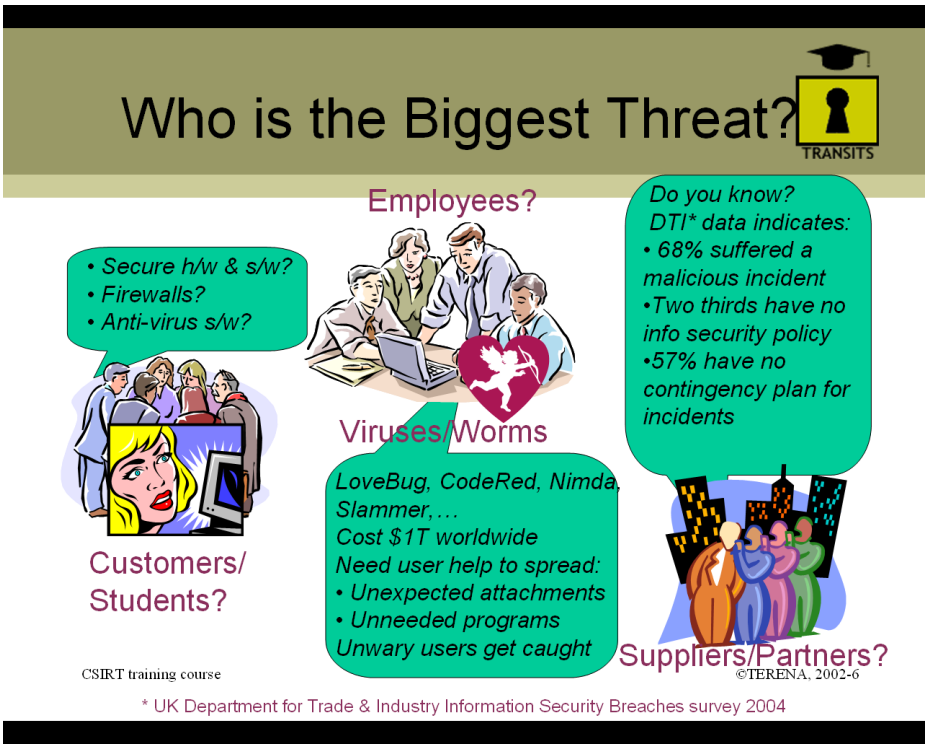
Pregled: Struktura tečaja



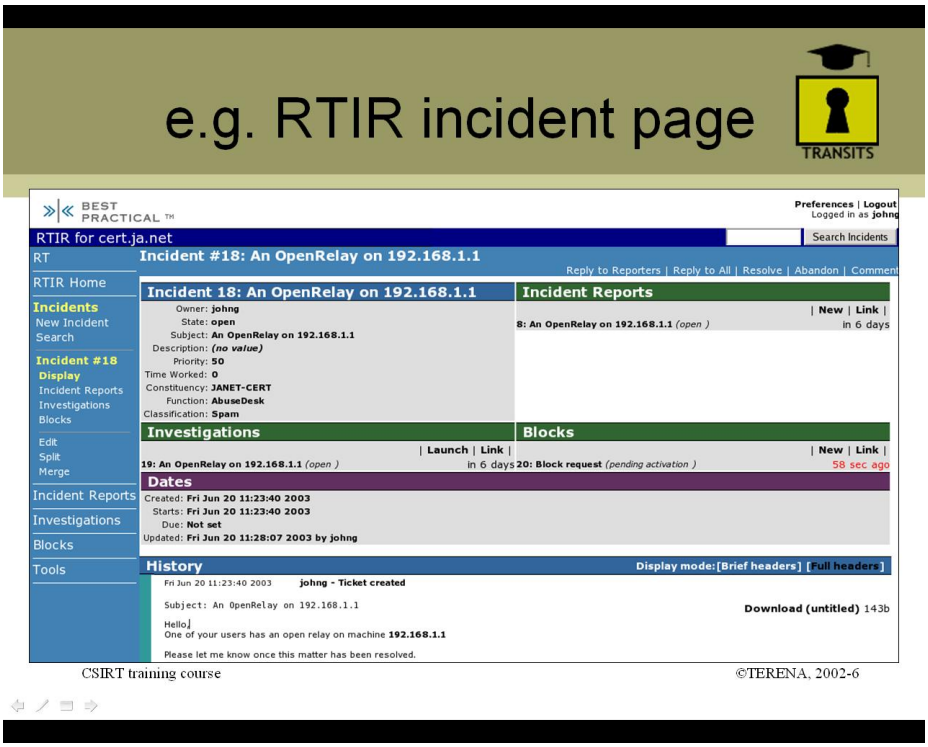
Iz *tehničnega modula*: Opis Botnet



Iz *tehničnega modula*: Osnovna zasnova orodij rootkit



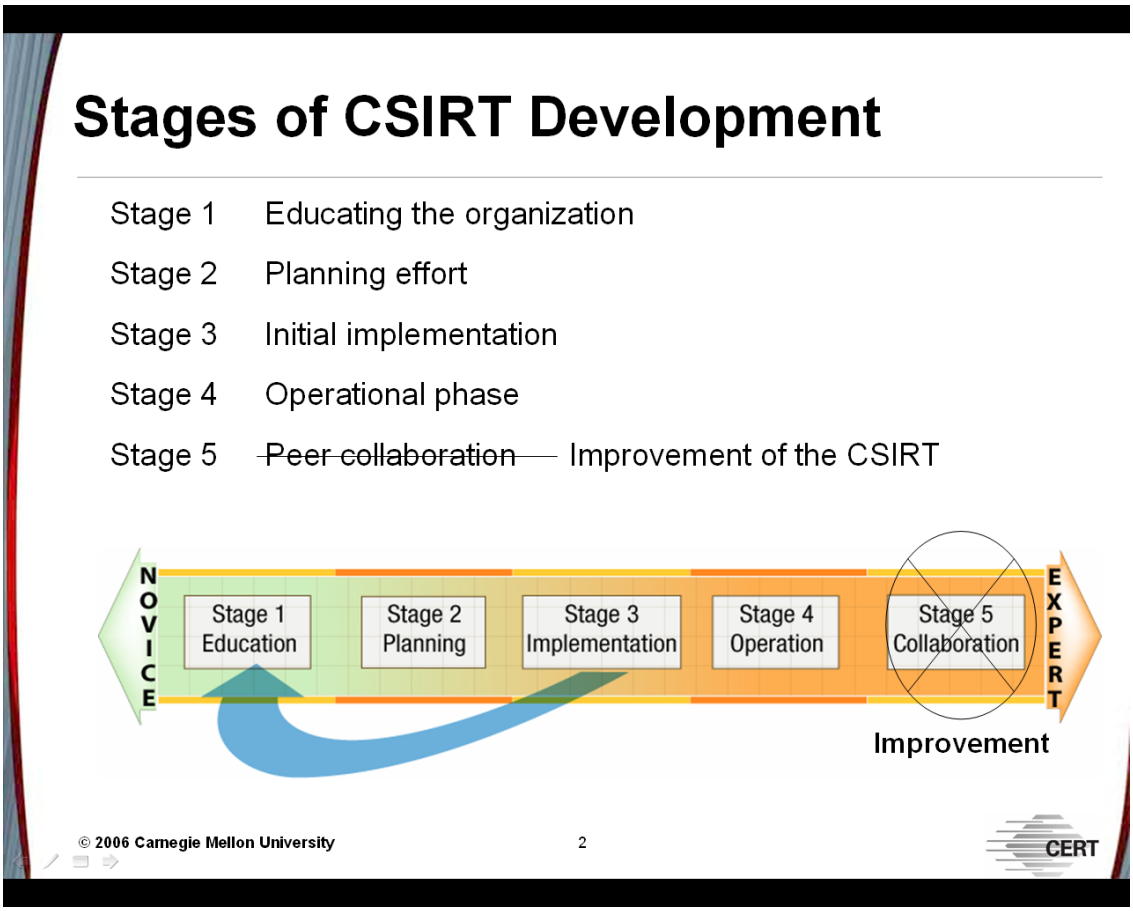
Iz *organizacijskega modula*: Oseba znotraj ali izven podjetja – kdo predstavlja večjo nevarnost?



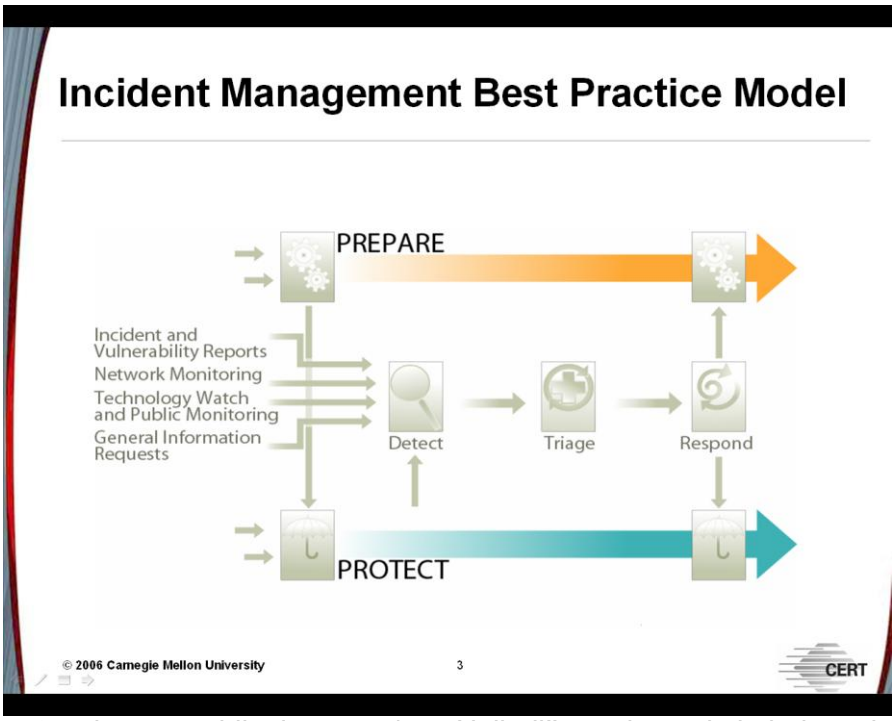
Iz *Operacijskega dela*: Zahteva v programu za sledenje odzivov na incident (RTIR)

„Vzpostavitev skupin CSIRT“ (z dovoljenjem za uporabo s strani CERT/CC, http://www.cert.org)

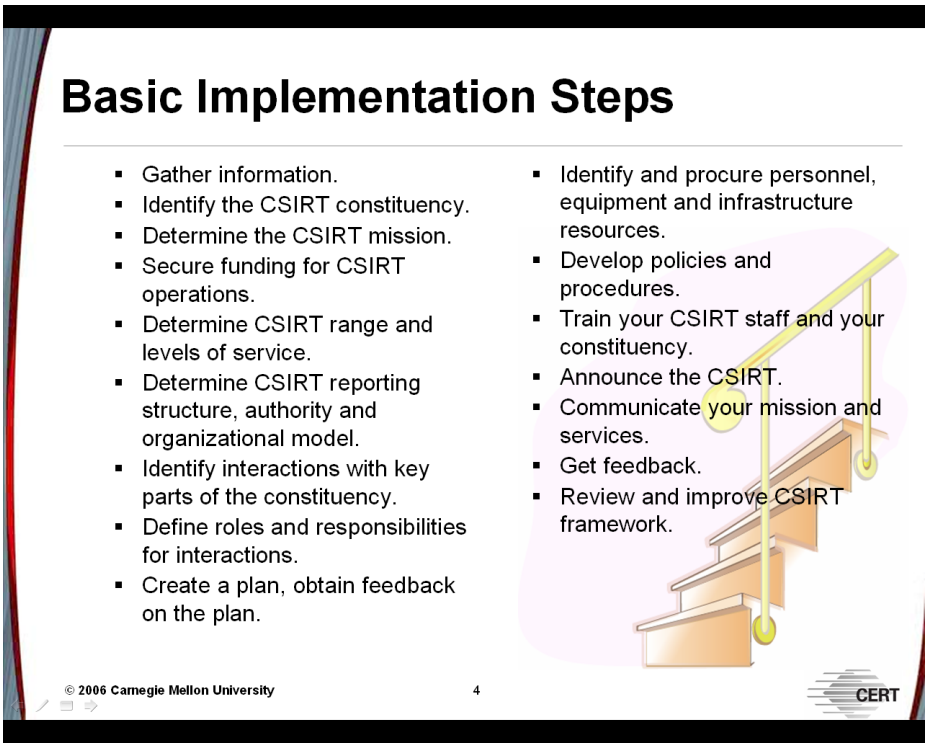
ENISA se zahvaljuje razvojni skupini CSIRT v programu CERT, ker nam je dovolila uporabo vsebine iz njihovih tečajev!



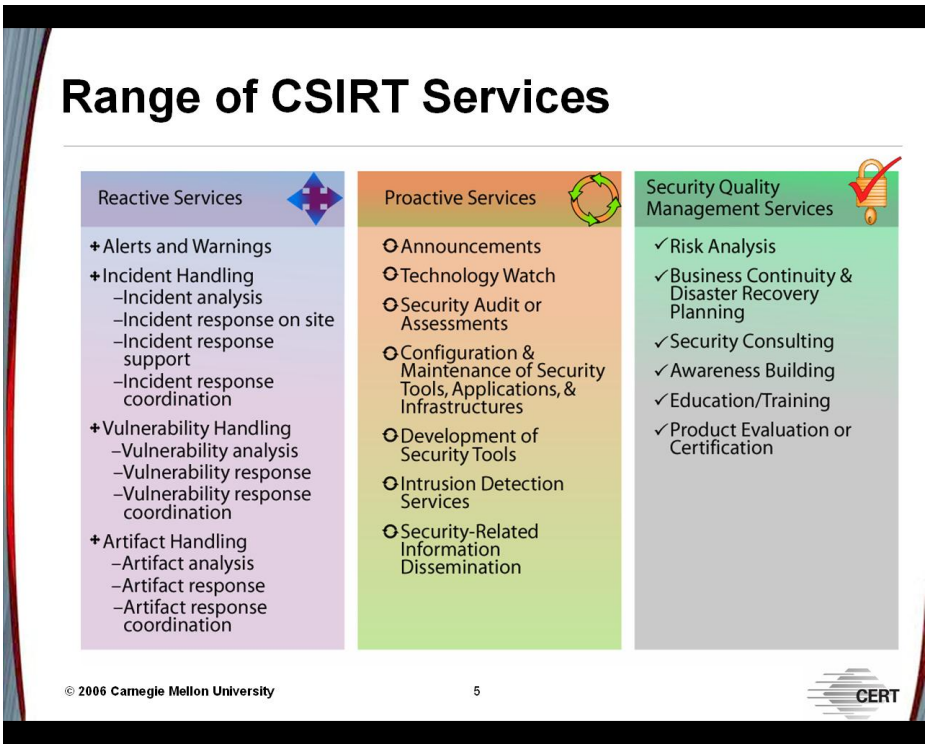
Iz *tečaja usposabljanja CERT/CC*: Faze razvoja skupine CSIRT



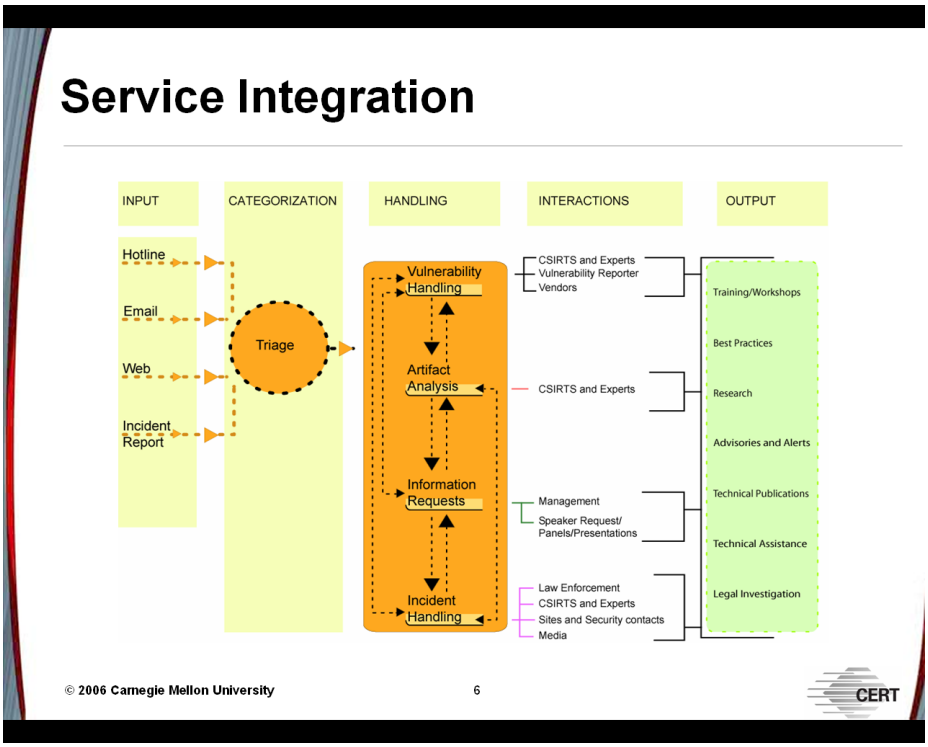
Iz *tečaja usposabljanja CERT/CC*: Najboljše prakse pri obvladovanju incidentov



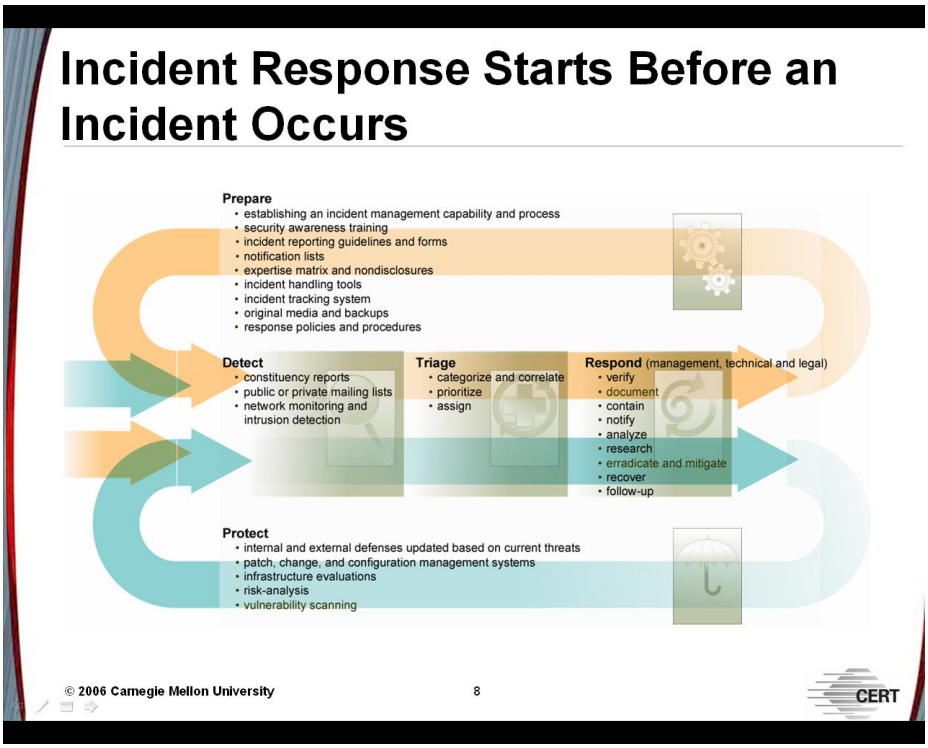
Iz *tečaja usposabljanja CERT/CC*: Koraki, ki jim je treba slediti pri vzpostavitvi skupine CSIRT



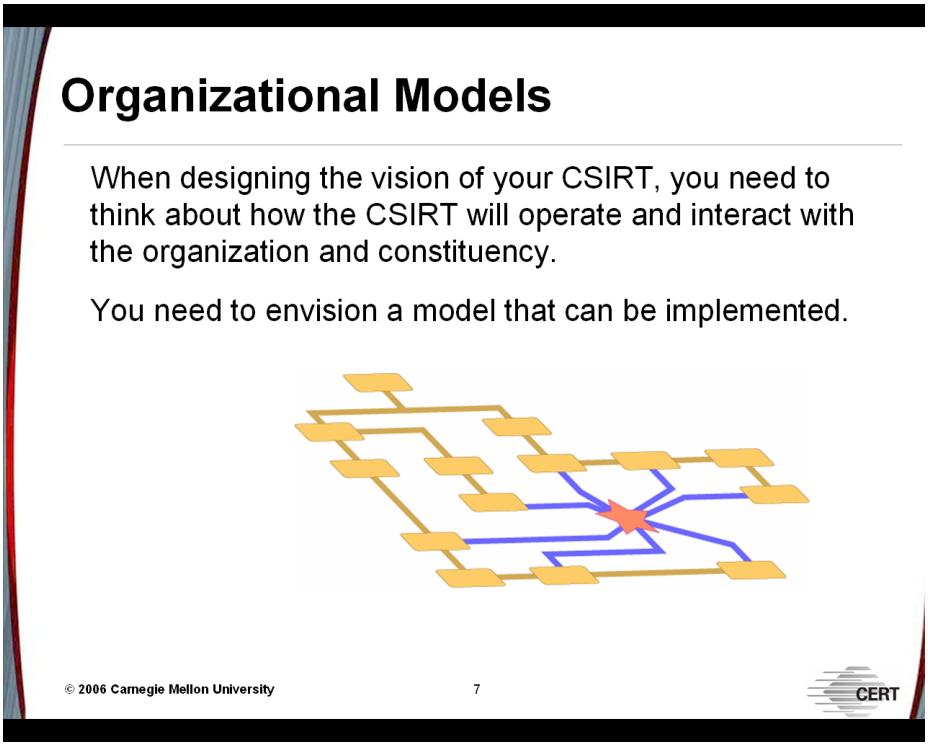
Iz *tečaja usposabljanja CERT/CC*: Storitve, ki jih lahko zagotavlja skupina CSIRT



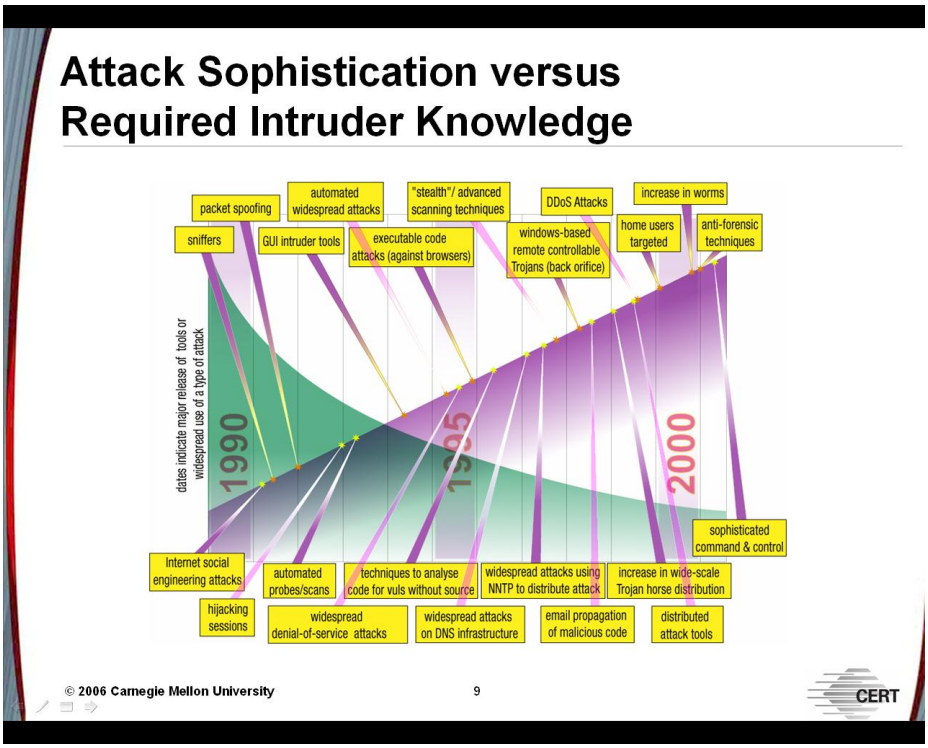
Iz *tečaja usposabljanja CERT/CC*: Potek dela pri obvladovanju incidentov



Iz *tečaja usposabljanja CERT/CC*: Odzivanje na incident



Iz *tečaja usposabljanja CERT/CC*: Kako bo organizirana skupina CSIRT?



Iz *tečaja usposabljanja CERT/CC*: Manj je znanja, večja je škoda