LAIPSNIŠKAS CSIRT GRUPĖS KŪRIMAS

Uždavinys, WP2006/5.1(CERT-D1/D2)

Rodyklė

1 Trumpas supažindinimas

Šiame dokumente apibūdinamas tinklų ir informacijos saugumo incidentų reagavimo grupės (angl. *Computer Security and Incident Response Team,* CSIRT) kūrimo procesas, atsižvelgiant į visus svarbius aspektus, pavyzdžiui, įmonės valdymo, procesų valdymo ir techninius. Šiuo dokumentu įgyvendinamas vienas iš dviejų 2006 m. ENISA darbo programos 5.1 skyriuje nurodytų uždavinių:

- Šis dokumentas – tai *raštiškas pranešimas apie laipsnišką CERT arba panašių struktūrų kūrimą, apimantis pavyzdžius*. (**CERT-D1**)
- 12 skyrius ir išoriniai dokumentai: *punktais suskirstytų gairių pavyzdys, kuriuo naudojantis gaires galima lengvai pritaikyti praktiškai.* (**CERT-D2**)

2 Teisinis pranešimas

Atkreipiame dėmesį į tai, kad šis leidinys atspindi autorių ir leidėjų požiūrį bei supratimą, jei nenurodyta kitaip. Šis leidinys neturėtų būti laikomas ENISA arba jos tarnybų veiksmu, nebent būtų priimtas pagal ENISA reglamentą (EB) Nr. 460/2004. Jis nebūtinai atspindi naujausią informaciją ir gali būti atnaujinamas.

Prireikus cituojami trečiųjų šalių šaltiniai. ENISA neatsako už trečiųjų šalių šaltinių, taip pat šiame leidinyje nurodytų trečiųjų šalių tinklaviečių turinį.

Jis skirtas tik šviesti ir informuoti. Nei ENISA, nei jos vardu veikiantys asmenys neatsako už galimą šiame leidinyje esančios informacijos panaudojimą.

3 Padėka

ENISA dėkoja visoms institucijoms ir asmenims, padėjusiems rengti šį dokumentą. Ypač norime padėkoti:

- konsultantui Henkui Bronkui, parengusiam pirmąją šio dokumento versiją,
- CERT/CC ir, ypač CSIRT kūrimo grupei, pateikusiai itin naudingą medžiagą ir priede pateiktą mokomojo kurso medžiagos pavyzdį,
- GovCERT.NL, pateikusiai *CERT-in-a-box,*
- TRANSITS grupei, pateikusiai mokomojo kurso medžiagos pavyzdį priede,
- Techninio departamento Saugumo skyriaus bendradarbiams, padėjusiems rengti 6.6 skyrių,
- visiems, peržiūrėjusiems šį dokumentą.

4 Įvadas

Ryšių tinklai ir informacijos sistemos tapo vienu svarbiausių ekonominės ir socialinės raidos veiksnių. Kompiuterinėmis ir ryšių tinklų paslaugomis taip pat plačiai naudojamasi kaip ir komunalinėmis elektros ar vandens tiekimo paslaugomis.

Todėl ryšių tinklų ir informacinių sistemų saugumas, ir ypač jų prieinamumas, kelia vis didėjantį visuomenės susirūpinimą. Taip yra todėl, kad dėl sistemos sudėtingumo, avarijų, klaidų ir įsilaužimų fizinės infrastruktūros, teikiančios ES piliečių gerovei ypač svarbias paslaugas, gali susidurti su svarbiausių informacinių sistemų problemomis.

2004 m. kovo 10 d. įsteigta Europos tinklų ir informacijos apsaugos agentūra (ENISA)[1]. Jos tikslas – užtikrinti aukštą ir veiksmingą Bendrijos tinklų ir informacijos saugumo lygį bei Europos Sąjungos piliečių, vartotojų, privataus ir valstybinio sektoriaus organizacijų labui kurti tinklų ir informacijos apsaugos kultūrą, taip skatinant sklandų vidaus rinkos funkcionavimą.

Jau kelerius metus, siekdamos saugesnio interneto, Europoje bendradarbiauja kelios saugos organizacijos, pavyzdžiui, CERT/CSIRT, kovos su piktnaudžiavimu tarnybos (angl. *Abuse Teams*) ir WARP. ENISA ketina remti šių organizacijų pastangas, teikdama informaciją apie tinkamo paslaugų kokybės lygio užtikrinimo priemones. Be to, ENISA ketina sustiprinti savo galimybes konsultuoti ES valstybes nares ir jos institucijas klausimais, susijusiais su tam tikroms IT vartotojų grupėms teikiamomis atitinkamomis saugumo paslaugomis. Todėl, remdamasi 2005 m. įkurtos specialiosios CERT bendradarbiavimo ir paramos darbo grupės išvadomis, naujoji darbo grupė nagrinės klausimus, susijusius su atitinkamų saugos paslaugų (CERT paslaugų) teikimu tam tikriems vartotojams (jų kategorijoms ar grupėms).

ENISA padeda kurti naujas CSIRT, išleisdama šį ENISA pranešimą „Laipsniškas CSIRT kūrimas, naudojant papildomą kontrolinį sąrašą“. Jis padės jums sukurti savo CSIRT.

[1] 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 460/2007, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą. Europos Bendrijos agentūra – tai ES įstaiga, skirta itin specifinėms techninėms, mokslinėms ar valdymo užduotims atlikti ES Bendrijos teisės (pirmojo ramsčio) srityje.

Tikslinė auditorija

Pagrindinės tikslinės šio pranešimo grupės yra vyriausybinės ir kitos institucijos, nusprendusios įkurti CSIRT, kad apsaugotų savo arba susijusių suinteresuotųjų asmenų IT infrastruktūrą.

Kaip naudotis šiuo dokumentu?

Šiame dokumente pateikiama informacija apie tai, kas yra CSIRT, kokias paslaugas ji gali teikti ir kokius pradinius žingsnius reikia žengti ją kuriant. Skaitytojui pateikiama CSIRT kūrimo metodų, jos struktūros ir turinio apžvalga.

4 skyrius: „Įvadas“
Šio pranešimo įvadas.

5 skyrius: „Bendroji CSIRT planavimo ir kūrimo strategija“.
Pirmame skirsnyje apibūdinama, kas yra CSIRT. Jame taip pat pateikiama informacijos apie aplinką, kurioje CSIRT gali veikti, ir apie paslaugas, kurias ji gali teikti.

6 skyrius: „Verslo plano kūrimas“.
Šiame skyriuje aprašomas įmonės vadovybės požiūris į kūrimo procesą.

7 skyrius: „Verslo plano rėmimas“.
Šiame skyriuje nagrinėjamas ekonominis modelis ir finansavimo klausimai.

8 skyrius: „Veiklos ir techninių procedūrų pavyzdžiai“.
Šiame skyriuje aprašoma informacijos gavimo ir jos talpinimo į saugos biuletenį procedūra. Jame taip pat apibūdinamas incidentų valdymo darbų srautas.

9 skyrius: „CSIRT mokymas“.
Šiame skyriuje apibendrinama informacija apie CSIRT darbuotojų mokymą. Priede pateiktas mokomojo kurso medžiagos pavyzdys.

10 skyrius: „Pratybos: informacinio biuletenio kūrimas“.
Šiame skyriuje pateikiamas pratimas, mokantis teikti vieną iš svarbiausių CSIRT paslaugų (arba pagrindinę CSIRT paslaugą), – kurti saugos (arba informacinį) biuletenį.

12 skyrius: „Veiklos projekto plano aprašymas“.
Šiame skyriuje nurodomas papildomas projekto planas (kontrolinis sąrašas), pateiktas kartu su šiuo vadovu. Siekiama, kad šis planas būtų lengvai naudojama šio vadovo įgyvendinimo priemonė.

Šio dokumento medžiagos pateikimo metodai

Kiekvieno skyriaus pradžioje apibendrinami jau žengti žingsniai CSIRT kūrimo procese. Apibendrinimai pateikiami tokiose lentelėse:

Žengėme pirmą žingsnį.

Kiekvienas skyrius baigiamas praktiniu aptartų priemonių įgyvendinimo pavyzdžiu. Šiame dokumente „Išgalvota CSIRT“ bus maža nepriklausoma vidutinės įmonės ar įstaigos CSIRT. Santrauka pateikiama priede.

Išgalvota CSIRT

5 Bendroji CSIRT planavimo ir kūrimo strategija

Norint sėkmingai pradėti CSIRT kūrimo procesą, svarbu aiškiai žinoti, kokias paslaugas grupė gali teikti savo klientams, „CSIRT pasaulyje“ geriau žinomais kaip „aptarnaujami subjektai“. Todėl būtina suprasti, kokie yra šių subjektų poreikiai, kad būtų galima teikti atitinkamas savalaikes ir kokybiškas paslaugas.

Kas yra CSIRT?

CSIRT – tai tinklų ir informacijos saugumo incidentų reagavimo grupė (angl. *Computer Security Incident Response Team*). Terminas CSIRT daugiausia naudojamas Europoje vietoje saugomo termino CERT, kurį JAV įregistravo CERT koordinavimo centras (angl. *CERT Coordination Center*).
Tos pačios rūšies terminams nusakyti yra naudojamos įvairios santrumpos:

- CERT arba CERT/CC (angl. *Computer Emergency Response Team / Coordination Center,* kompiuterinių incidentų tyrimo tarnyba/koordinavimo centras),
- CSIRT (angl. *Computer Security Incident Response Team,* tinklų ir informacijos saugumo incidentų reagavimo grupė),
- IRT (angl. *Incident Response Team,* incidentų reagavimo grupė),
- CIRT (angl. *Computer Incident Response Team,* kompiuterinių incidentų reagavimo grupė),
- SERT (angl. *Security Emergency Response Team,* saugumo incidentų tyrimo tarnyba).

Pastarojo amžiaus devintojo dešimtmečio pabaigoje IT infrastruktūroje kilo pirmas didelio masto „kompiuterinio kirmino“ proveržis. Morisu pavadintas kirminas[2] greitai pasklido visame pasaulyje ir sutrikdė daugelio IT sistemų veiklą.

Šis incidentas buvo tarsi žadintuvo skambutis: staiga žmonės suvokė, jog sistemų administratoriams ir IT vadovams būtina bendradarbiauti ir derinti savo veiklą, kad būtų galima spręsti tokias problemas, kaip ši. Kadangi esminis veiksnys buvo laikas, reikėjo rasti geriau organizuotų ir struktūrinių IT saugumo incidentų valdymo priemonių. Todėl, praėjus kelioms dienoms po „Moriso incidento“, Pažangių tyrimų projektų agentūra (angl. *Defence Advanced Research Projects Agency,* DARPA) įkūrė pirmąją CSIRT – CERT koordinavimo centrą (CERT/CC[3]), įsikūrusį Karnegio Melono universitete *(*angl. *Carnegie Mellon University)* Pitsburge (Pensilvanijos valstijoje).

Šis modelis netrukus buvo pritaikytas Europoje, ir 1992 m. olandų akademinių paslaugų teikėjas SURF*net* Europoje įkūrė pirmą CSIRT, pavadintą SURFnet-CERT[4]. Po to buvo sudaryta daug grupių, ir šiuo metu ENISA „CERT veiklos Europoje[5] apžvalgoje“ yra nurodyta daugiau kaip 100 žinomų Europoje įsikūrusių grupių.

[2] Išsamesnės informacijos apie kirminą Morisą galima rasti adresu: http://en.wikipedia.org/wiki/Morris_worm.

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

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

[5] ENISA „Apžvalga“: http://www.enisa.europa.eu/cert_inventory/

Laikui bėgant CERT grupės išplėtė savo pajėgumus nuo tik reagavimo pajėgų iki visų apsaugos paslaugų teikėjo, įskaitant prevencines paslaugas, pavyzdžiui, įspėjimus, saugos biuletenius, mokymo ir saugos valdymo paslaugas. Netrukus nuspręsta, kad terminas „CERT“ nepakankamai platus. Todėl pastarojo amžiaus dešimtojo dešimtmečio pabaigoje apibrėžtas naujas terminas – CSIRT. Šiuo metu abu terminai (CERT ir CSIRT) naudojami kaip sinonimai, tačiau CSIRT yra tikslesnis.

5..1 Terminas „aptarnaujami subjektai“

Toliau (CSIRT bendrijose) nurodant CSIRT užsakovų bazę, bus naudojamas gerai žinomas terminas „aptarnaujami subjektai“. Paskiras užsakovas bus vadinamas „aptarnaujamu subjektu“, o grupė – „aptarnaujamais subjektais“.

5..2 CSIRT apibrėžimas

CSIRT – tai IT saugos specialistų grupė, kurios pagrindinė veikla – reaguoti į tinklų ir informacijos saugos incidentus. Ji teikia būtinas paslaugas jiems valdyti ir padeda savo aptarnaujamiems subjektams susidoroti su pažeidimų padariniais.

Siekdamos sušvelninti riziką ir sumažinti būtino reagavimo atvejų skaičių, daugelis CSIRT grupių savo aptarnaujamiems subjektams taip pat teikia prevencijos ir švietimo paslaugas. Jos leidžia biuletenius apie naudojamos programinės ir aparatinės įrangos trūkumus, taip pat informuoja vartotojus apie jų pažeidžiamumą išnaudojančias programas ir šiais trūkumais pasinaudojančius virusus. Tai padeda aptarnaujamiems subjektams greitai pataisyti ir atnaujinti savo sistemas. Visą galimų paslaugų sąrašą rasite 5.2 skyriuje „Paslaugos“.

5..3 CSIRT nauda

Turėdama specializuotą IT saugos specialistų grupę, organizacija gali sumažinti incidentų skaičių ir vykdyti jų prevenciją ir taip apsaugoti vertingą savo turtą.

Kita galima nauda:

- Centralizuotas IT apsaugos aspektų koordinavimas organizacijoje (informacijos teikimo vieta (ITV)).
- Centralizuotas ir specializuotas IT incidentų valdymas ir reagavimas į juos.
- Čia pat esantys specialistai pataria ir padeda vartotojams greitai atitaisyti saugumo incidentų padarinius.
- Teismo proceso atveju sprendžiami teisiniai klausimus ir saugomi įrodymai.
- Turima tikslios naujausios informacijos apie pasiekimus saugos srityje.
- Skatinamas aptarnaujamų subjektų bendradarbiavimas IT saugos srityje (sąmoningumo skatinimas).

•

Išgalvota CSIRT (0 žingsnis)
Suprasti, kas yra CSIRT Pavyzdžiui, pavyzdinė CSIRT turės teikti paslaugas vidutinei įstaigai, kurioje dirba iki 200 darbuotojų. Įstaiga turi savo IT skyrių ir du filialus toje pačioje šalyje. IT sistema įmonei itin svarbi, kadangi ji naudojama vidaus ryšiams, duomenų tinklui ir visą parą bei septynias dienas per savaitę (24x7) veikiančiam elektroniniam verslui. Įstaiga turi savo tinklą ir naudojasi dviejų interneto paslaugų teikėjų (ISP) teikiama prieiga prie interneto.

5..4 Įvairių tipų CSIRT aplinkos apibūdinimas

Žengėme pirmą žingsnį.

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.

>> Kitas žingsnis – rasti atsakymą į klausimą: „Kokiam sektoriui bus teikiamos CSIRT paslaugos?“

Steigiant CSIRT (kaip bet kokią kitą įmonę), labai svarbu greitai aiškiai nustatyti, kas yra jos aptarnaujami subjektai ir kokioje aplinkoje bus teikiamos CSIRT paslaugos. Šiuo metu galima išskirti šiuos abėcėlės tvarka išdėstytus „sektorius“:

- Akademinio sektoriaus CSIRT
- Komercinė CSIRT
- CIP/CIIP sektoriaus CSIRT
- Vyriausybinio sektoriaus CSIRT
- Vidaus CSIRT
- Karinio sektoriaus CSIRT
- Nacionalinė CSIRT
- Mažų ir vidutinių įmonių (MVĮ) sektoriaus CSIRT
- Gamintojų CSIRT

Akademinio sektoriaus CSIRT
Veiklos sritis
Akademinio sektoriaus CSIRT teikia paslaugas akademinėms ir švietimo įstaigoms, pavyzdžiui, universitetams ar jų tyrimo infrastruktūrai, ir jų teritorijų interneto aplinkai.

Aptarnaujami subjektai
Paprastai šios CSIRT paslaugos teikiamos universitetų darbuotojams ir studentams.

Komercinė CSIRT
Veiklos sritis
Komercinė CSIRT savo aptarnaujamiems subjektams paslaugas teikia komerciniu pagrindu. ISP atveju galutiniams klientams CSIRT dažniausiai teikia kovos su piktnaudžiavimu paslaugas (Dial-in, ADSL) ir CSIRT paslaugas savo profesionaliems klientams.

Aptarnaujami subjektai
Komercinės CSIRT paprastai savo paslaugas teikia tiems aptarnaujamiems subjektams, kurie už jas moka.

CIP/CIIP sektoriaus CSIRT

Veiklos sritis

Šiame sektoriuje CSIRT grupės pagrindinį dėmesį skiria ypatingos svarbos informacijos (angl. *Critical Information Protection* (CIP)) ir (arba) ypatingos svarbos informacijos ir infrastruktūros objektų apsaugai (angl. *Critical Information and Infrastructure protection* (CIIP). Daugeliu atveju ši specializuota CSIRT glaudžiai bendradarbiauja su vyriausybiniu CIIP departamentu. Jis apima visus šalies ypatingos svarbos IT sektorius ir saugo piliečius.

Aptarnaujami subjektai

Vyriausybė, ypatingos svarbos IT įmonės, piliečiai.

Vyriausybinio sektoriaus CSIRT

Veiklos sritis

Vyriausybinė CSIRT grupė teikia paslaugas vyriausybinėms agentūroms ir, kai kuriose šalyse, piliečiams.

Aptarnaujami subjektai

Vyriausybė ir su ja susijusios agentūros. Kai kuriose šalyse įspėjimo paslaugos teikiamos ir piliečiams (pvz., Belgijoje, Vengrijoje, Nyderlanduose, Jungtinėje Karalystėje ar Vokietijoje).

Vidaus CSIRT

Veiklos sritis

Vidaus CSIRT teikia paslaugas tik savo pagrindinei organizacijai. Tai galima apibūdinti daugiau kaip veikimo principą, o ne sektorių. Pavyzdžiui, daug telekomunikacijų įmonių ir bankų turi įsteigę savo vidines CSIRT grupes. Visuomenei skirtos tinklavietės jos dažniausiai neturi.

Aptarnaujami subjektai

Pagrindinės įmonės vidaus darbuotojai ir IT skyrius.

Karinio sektoriaus CSIRT

Veiklos sritis

Šio sektoriaus CSIRT paslaugas teikia karinėms organizacijoms, atsakingoms už gynybos tikslams skirtą IT infrastruktūrą.

Aptarnaujami subjektai

Karinių įstaigų arba atitinkamų įmonių, pavyzdžiui, Gynybos departamento, darbuotojams.

Nacionalinė CSIRT

Veiklos sritis

Nacionaliniams poreikiams skirta CSIRT laikoma šalies saugumo informacijos teikimo vieta. Kai kuriais atvejais vyriausybinė CSIRT taip pat veikia kaip šalies ITV (kaip UNIRAS Jungtinėje Karalystėje).

Aptarnaujami subjektai

Šio tipo CSIRT dažniausiai neturi tiesioginių aptarnaujamų subjektų, kadangi nacionalinė CSIRT šalyje atlieka tik tarpininko vaidmenį.

Mažų ir vidutinių įmonių (MVĮ) sektoriaus CSIRT
Veiklos sritis
Pačių įmonių suburta CSIRT teikia paslaugas savo verslo šakos ar panašių vartotojų grupei.

Aptarnaujami subjektai
Šių CSIRT aptarnaujami subjektai gali būti MVĮ ir jų darbuotojai arba tam tikrų interesų grupės, pavyzdžiui, šalies administracinių centrų ir savivaldybių asociacijos.

Gamintojų CSIRT
Veiklos sritis
Gamintojų CSIRT dėmesį skiria specifiniams gamintojų produktams remti. Dažniausiai jos siekia rasti ir teikti sprendimus, siekiant pašalinti trūkumus ir sumažinti galimą neigiamą jų poveikį.

Aptarnaujami subjektai
Produktų savininkai.

Kaip apibūdinta dalyje apie nacionalines CSIRT, grupė gali teikti paslaugas daugiau nei vienam sektoriui. Tai turi poveikį, pavyzdžiui, aptarnaujamų subjektų ir jų poreikių analizei.

Išgalvota CSIRT (1 žingsnis)
Pradinis etapas Pradiniame etape nauja CSIRT planuojama kaip vidaus CSIRT, teikianti paslaugas pagrindinei įmonei, vietiniam IT skyriui ir darbuotojams. Ji taip pat remia ir koordinuoja su IT saugumu susijusių incidentų valdymą įvairiuose filialuose.

CSIRT teikiamos paslaugos

Žengėme pirmus du žingsnius.

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.
2. Nustatėme, kokiam sektoriui nauja grupė teiks savo paslaugas.

Kitas žingsnis – atsakyti į klausimą, *kokias paslaugas teikti aptarnaujamiems subjektams*.

CSIRT gali teikti įvairių rūšių paslaugas, tačiau iki šiol nė viena neteikia visų. Todėl tinkamo paslaugų paketo pasirinkimas yra lemiamas sprendimas. Toliau rasite trumpą

visų žinomų CSIRT paslaugų, apibrėžtų CERT/CC[6] išleistoje „CSIRT grupių atmintinėje“, apžvalgą.

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

Reaktyviosios paslaugos	**Iniciatyviosios paslaugos**	**Artefaktų valdymas**
• **Perspėjimai ir įspėjimai** • **Incidentų valdymas** • **Incidentų analizė** • **Reagavimo į incidentus pagalba** • **Reagavimo į incidentus koordinavimas** • Reagavimas į incidentus vietoje • Pažeidžiamumo valdymas • Pažeidžiamumo analizė • Reagavimas į pažeidžiamumą • Reagavimo į pažeidžiamumą koordinavimas	• **Pranešimai** • Technologijos naujovių sekimas • Saugos auditas arba vertinimas • Apsaugos konfigūravimas ir priežiūra • Apsaugos priemonių tobulinimas • Įsibrovimo aptikimo paslaugos • Su sauga susijusios informacijos skleidimas	• *Artefaktų analizė* • *Reagavimas į artefaktus* • *Reagavimo į artefaktus koordinavimas* ***Apsaugos kokybės valdymas*** • *Rizikos analizė* • *Verslo tęstinumas ir sutrikimo padarinių šalinimas* • *Konsultavimas saugos klausimais* • *Informacijos skleidimas* • *Švietimas/mokymas* • *Produkto vertinimas arba sertifikavimas*

1 pav. CERT/CC sudarytas CSIRT paslaugų sąrašas [7].

Pagrindinės paslaugos (užrašytos pastorintu šriftu): reaktyviosios ir iniciatyviosios paslaugos skiriasi. Iniciatyviosios paslaugos skirtos incidentų prevencijai skleidžiant informaciją ir mokant, o reaktyviųjų paslaugų paskirtis – valdyti incidentus ir sušvelninti jų žalą.

Artefaktų valdymas apima visų sistemoje aptinkamų failų ar objektų, pvz., virusų likučių, kirminų, grafinių ženklų, Trojos arklių, ir kt., kurie galėtų būti naudojami piktavalei veiklai, analizę. Jis taip pat apima gautos informacijos tvarkymą ir jos perdavimą gamintojams bei kitoms suinteresuotoms šalims, siekiant užkirsti kelią tolesniam „kenkėjiškos“ programos plitimui ir sumažinti riziką.

Apsaugos ir kokybės valdymo paslaugos – tai konsultavimo ir švietimo priemones apimančios paslaugos, kuriomis siekiama ilgalaikių tikslų.

Išsamų CSIRT paslaugų paaiškinimą galima rasti priede.

Tinkamų paslaugų parinkimas savo aptarnaujamiems subjektams yra svarbus žingsnis. Išsamiau apie jį kalbama 6.1 skyriuje „Finansinio modelio nustatymas“.

Dauguma CSIRT grupių savo veiklą pradeda savo aptarnaujamiems subjektams siųsdamos perspėjimus ir įspėjimus, rašydamos pranešimus ir užsiimdamos incidentų valdymu. Dažniausiai šios pagrindinės paslaugos atkreipia aptarnaujamų subjektų dėmesį ir yra jų vertinamos, ir dažniausiai yra laikomos tikra „pridėtine verte“.

[7] CERT/CC sudarytas CSIRT paslaugų sąrašas: http://www.cert.org/csirts/services.html

Veiklą labai naudinga pradėti sudarant mažą „bandomųjų“ aptarnaujamų subjektų grupę, pagrindines paslaugas teikti nustatytu bandomuoju laikotarpiu, o jam pasibaigus – paprašyti pateikti atsiliepimų.
Suinteresuoti bandomieji vartotojai paprastai pateikia konstruktyvius atsiliepimus ir padeda tobulinti individualias paslaugas.

Išgalvota CSIRT (2 žingsnis)
Tinkamų paslaugų pasirinkimas Pradiniame etape nutariama, kad naujoji CSIRT daugiausia dėmesio teiks tam tikrų pagrindinių paslaugų teikimui. Nusprendžiama, kad pasibaigus bandomajam etapui, gali būti svarstoma, ar nereikėtų papildyti paslaugų paketo, ir gali būti pridedamos tam tikros apsaugos valdymo paslaugos. Toks sprendimas priimamas remiantis bandomųjų aptarnaujamų subjektų atsiliepimais ir glaudžiai bendradarbiaujant su Kokybės užtikrinimo skyriumi.

Aptarnaujamų subjektų analizė ir veiklos apibrėžimas

Žengėme pirmus tris žingsnius:

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.
2. Nustatėme, kokiam sektoriui nauja grupė teiks savo paslaugas.
3. Aptarėme paslaugas, kurias CSIRT gali teikti savo aptarnaujamiems subjektams.

>> Kitas žingsnis – atsakyti į klausimą, *kokį CSIRT kūrimo metodą pasirinkti?*

Tolesnis žingsnis – tai atidesnis žvilgsnis į aptarnaujamus subjektus, siekiant pasirinkti tinkamus ryšių kanalus.

- Ryšių su klientais palaikymo metodo nustatymas.
- Veiklos apibrėžimas
- Realaus įgyvendinimo/veiklos projekto plano sudarymas.
- CSIRT paslaugų nustatymas.
- Organizacinės struktūros apibrėžimas.
- Informacijos apsaugos politikos apibūdinimas
- Tinkamų darbuotojų samdymas.
- CSIRT biuro panaudojimas.
- Bendradarbiavimo su kitomis CSIRT galimybių ir galimų nacionalinių iniciatyvų ieškojimas.

Tolesnėse dalyse šie žingsniai bus aprašyti išsamiau, ir gali būti naudojami verslo ir veiklos projekto planams sudaryti.

5..1 Ryšių su aptarnaujamais subjektais metodas

Kaip pasakyta anksčiau, labai svarbu žinoti aptarnaujamų subjektų poreikius, taip pat savo ryšių strategiją, įskaitant ryšių kanalus, labiausiai tinkančius teikti jiems informaciją.

Valdymo teorijoje žinomi keli galimi tikslinės grupės analizės būdai. Šiame dokumente aprašyti du: SWOT ir PEST analizė.

SWOT analizė
SWOT analizė yra strateginio planavimo priemonė, skirta vertinti projekto, įmonės ar kito atvejo, kuriam reikia priimti sprendimą, privalumus, trūkumus, galimybes ir grėsmes (angl. ***S****trengths,* ***W****eaknesses,* ***O****pportunities, and* ***T****hreats*). Metodas priskiriamas *Albert'ui Humphre'iui*, kuris praeito amžiaus septintajame ir aštuntajame dešimtmetyje Stanfordo universitete vadovavo tyrimo projektui, kuriam naudojo žurnale „Fortune 500“ minimų bendrovių duomenis.[8]

Privalumai	**Trūkumai**
Galimybės	**Grėsmės**

2 pav. SWOT analizė.

[8] SWOT analizės aiškinimas „Vikipedijoje“ (*Wikipedia)*: http://en.wikipedia.org/wiki/SWOT_analysis

PEST analizė

PEST analizė yra kita svarbi ir plačiai naudojama aptarnaujamų subjektų analizės priemonė, padedanti suprasti aplinkos, kurioje veikia CSIRT, politines, ekonomines, socialines ir kultūrines bei technologines sąlygas (angl. ***P**olitical, **E**conomic, **S**ocio-cultural and **T**echnological*).

Politinės	**Ekonominės**
• Politiniai/aplinkosauginiai aspektai • Atitinkamoje šalyje galiojantys teisės aktai • Būsimi teisės aktai • Europos/tarptautiniai teisės aktai • Reguliavimo institucijos ir procesai • Vyriausybės politikos sritys • Vyriausybės kadencijos trukmė ir kaita • Prekybos politika • Finansavimas, subsidijos ir iniciatyvos • Vidaus rinkos lobistų/suinteresuotų asmenų grupės • Tarptautinės lobistų grupės	• Vidaus ekonominė padėtis • Vidaus ekonomikos tendencijos • Užsienio šalių ekonomika ir tendencijos • Bendrieji mokesčių aspektai • Konkrečių produktų/paslaugų apmokestinimas • Sezoniškumas/klimato aspektai • Rinkos ir prekybos ciklai • Specifiniai verslo šakos veiksniai • Rinkos srautai ir paskirstymo tendencijos • Kliento/galutinio vartotojo paskatos • Palūkanų normos ir valiutų kursas
Socialinės	**Technologinės**
• Gyvenimo būdo tendencijos • Demografiniai duomenys • Vartotojų požiūris ir nuomonė • Žiniasklaidos požiūris • Įstatymų pokyčiai, turintys poveikį socialiniams veiksniams • Prekės ženklo, įmonės, technologijos įvaizdis • Vartotojų pirkimo įpročiai • Stilius ir sektini pavyzdžiai • Pagrindiniai įvykiai ir įtaka • Pirkimo prieiga ir tendencijos • Etniniai/religiniai veiksniai • Reklama ir viešumas	• Konkuruojančių technologijų plėtra • Mokslinių tyrimų finansavimas • Susijusios/pavaldžios technologijos • Pakaitinės technologijos/sprendimai • Technologijos užbaigtumas • Gamybos užbaigtumas ir pajėgumas • Informacija ir komunikacijos • Vartotojų pirkimo mechanizmai/technologija • Technologijos teisės aktai • Naujovių kūrimo pajėgumas • Technologijos prieiga, licencijavimas, patentai • Intelektinės nuosavybės aspektai

3 pav. PEST analizės modelis.

Išsamų PEST analizės aprašymą galima rasti „Vikipedijoje“ (Wikipedia[9]).
Abi priemonės leidžia visapusiškai ir struktūriškai apžvelgti aptarnaujamų subjektų poreikius. Rezultatai papildo verslo pasiūlymą ir taip padeda gauti finansavimą CSIRT steigti.

Ryšių kanalai

Svarbi analizės tema yra galimi ryšių ir informacijos teikimo metodai („Kaip bendrauti su aptarnaujamais subjektais?“).

Jei įmanoma, būtina apsvarstyti nuolat rengiamų asmeninių aptarnaujamų subjektų apsilankymų galimybę. Įrodyta, kad tiesioginiai susitikimai palengvina bendradarbiavimą. Jei abi šalys nori dirbti kartu, šie susitikimai padeda puoselėti atviresnius santykius.

[9] PEST analizė „Vikipedijoje“ (*Wikipedia*): http://en.wikipedia.org/wiki/PEST_analysis

Paprastai CSIRT turi kelis ryšių kanalus. Verta pagalvoti apie šiuos kanalus, kadangi jie pasirodė esą naudingi:

- Vieša tinklavietė
- Uždara tinklavietės narių sritis
- Elektroniniai blankai pranešimams apie incidentus skelbti
- Adresatų sąrašai
- Konkretaus asmens el. paštas
- Telefonas/faksas
- Tekstinės žinutės (SMS)
- „Senamadiški“ popieriniai laiškai
- Mėnesinės arba metinės ataskaitos

Be el. pašto, el. blankų, telefono ar fakso, naudojamų palengvinti incidento tyrimą (gauti aptarnaujamų subjektų pranešimus apie incidentus, derinti veiksmus su kitomis grupėmis ar teikti atsiliepimus ir pagalbą nukentėjusiajam), dauguma CSIRT patarimus saugos klausimais skelbia viešose tinklavietėse ir naudodami adresatų sąrašus.

! Jei įmanoma, informacija turi būti skleidžiama saugiai. Pavyzdžiui, el. laiškas gali būti pasirašomas skaitmeniniu būdu, naudojantis *PGP* (angl. *Pretty Good Privacy*), o slapti incidento duomenys visada turi būti siunčiami užšifruoti.

Išsamesnės informacijos rasite 8.5 skyriuje „CSIRT naudojamos priemonės“. Taip pat žiūrėkite *RFC2350 2.3* skyrių[10].

Išgalvota CSIRT (3a žingsnis)

Aptarnaujamų subjektų ir atitinkamų ryšio kanalų analizė

Kolektyvinis posėdis su kai kuriais pagrindiniais vadovybės ir aptarnaujamų subjektų asmenimis pakankamai prisidėjo atliekant SWOT analizę. Padaryta išvada, kad būtinos šios pagrindinės paslaugos:

- Perspėjimai ir įspėjimai
- Incidentų valdymas (analizė, reagavimo pagalba ir reagavimo koordinavimas)
- Pranešimai

Būtina užtikrinti, kad informacijos skleidimas būtų gerai organizuotas, kad pasiektų kuo didesnę aptarnaujamų subjektų dalį. Taigi nusprendžiama, kad perspėjimai, įspėjimai ir pranešimai saugos biuletenių forma bus skelbiami specialioje tinklavietėje ir platinami naudojant adresatų sąrašą. CSIRT palengvina pranešimų apie incidentus gavimą el. paštu, telefonu ir faksu. Kitame žingsnyje planuojamas vienodos formos el. blankas

SWOT analizės pavyzdį žiūrėkite kitame puslapyje.

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

Privalumai • Įmonė turi kai kurių žinių • Darbuotojams patinka planas ir jie nori bendradarbiauti • Administracijos valdybos parama ir finansavimas	**Trūkumai** • Nepakankamas įvairių skyrių ir filialų bendravimas • Nederinama veikla IT incidentų atžvilgiu • Daug „mažų skyrių“
Galimybės • Didelis struktūriškai neapibrėžto pažeidžiamumo informacijos srautas • Būtinas veiksmų derinimas • Dėl incidentų patiriamų nuostolių mažinimas • Daug neišspręstų klausimų IT apsaugos srityje • IT apsaugos mokomasis personalas	**Grėsmės** • Nedaug pinigų • Mažai darbuotojų • Dideli lūkesčiai • Kultūra

4 pav. SWOT analizės pavyzdys.

5..2 Veiklos apibrėžimas

Išanalizavus aptarnaujamų subjektų poreikius ir norus dėl CSIRT paslaugų, kitas žingsnis yra apibrėžti jos veiklą.

Apibrėžiant veiklą apibūdinama pagrindinė organizacijos funkcija visuomenėje, nurodant aptarnaujamiems subjektams teikiamus produktus ir paslaugas. Ji suteikia galimybę aiškiai pranešti apie naujos CSIRT egzistavimą ir funkcijas.

Veiklą naudinga išdėstyti trumpai, bet ne per daug glaustai, kadangi dažniausiai ji nekinta kelerius metus.

Štai keli veikiančių CSIRT veiklos apibrėžimo pavyzdžiai:

„<CSIRT pavadinimas> savo <aptarnaujamiems subjektams (apibrėžkite savo aptarnaujamus subjektus)> teikia informaciją ir pagalbą, taikydama iniciatyviąsias priemones, skirtas tinklų ir informacijos saugumo incidentų rizikai mažinti, taip pat reaguoja į tokius incidentus jiems kilus“.
„Padėti <aptarnaujamiems subjektams> užkirsti kelią su IT susijusiems saugumo incidentams ir reaguoti į juos“.[11]

[11] *Govcert.nl* paskirties formulavimas: http://www.govcert.nl

Veiklos apibrėžimas yra labai svarbus ir būtinas pradinis žingsnis. *RFC2350*[12] *2.1* skyriuje rasite išsamesnį apibūdinimą, kokią informaciją CSIRT turėtų skelbti.

Išgalvota CSIRT (3b žingsnis)
Išgalvotos CSIRT vadovybė veiklą apibrėžė taip: *„Išgalvota CSIRT savo pagrindinės įmonės darbuotojams teikia informaciją ir padeda mažinti tinklų ir informacijos saugumo incidentų riziką, taip pat reaguoja į tokius incidentus, jiems kilus“.* Šia formuluote išgalvota CSIRT aiškiai pasako, kad ji yra vidinė CSIRT, kurios pagrindinė veikla – spręsti su IT sauga susijusius klausimus.

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

6 Verslo plano kūrimas

Žengėme šiuos žingsnius:

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.
2. Nustatėme, kokiam sektoriui nauja grupė teiks savo paslaugas.
3. Aptarėme paslaugas, kurias CSIRT gali teikti savo aptarnaujamiems subjektams.
4. Išanalizavome aplinką ir klientus
5. Apibrėžėme veiklą.

>> Kitas žingsnis yra apibrėžti verslo planą.

Analizės rezultatai gerai nušviečia aptarnaujamų subjektų poreikius ir (numanomus) trūkumus, taigi jais remiamasi kitame žingsnyje.

Finansinio modelio nustatymas

Atlikus analizę, pradžiai pasirinktos kelios pagrindinės paslaugos. Kitas žingsnis – apgalvoti finansinį modelį: kokie paslaugos teikimo kriterijai yra tinkami ir apsimoka.

Tobulame pasaulyje finansavimas būtų pritaikytas aptarnaujamų subjektų poreikiams, tačiau tikrovėje galimų teikti paslaugų paketas turi būti pritaikytas prie turimo biudžeto. Todėl praktiškiau pradėti nuo piniginių aspektų planavimo.

6..1 Išlaidų modelis

Du pagrindiniai išlaidas lemiantys veiksniai yra paslaugų teikimo valandų ir darbuotojų skaičiaus (bei kvalifikacijos) nustatymas. Ar reagavimo į incidentus ir techninės pagalbos paslaugas būtina teikti 24 valandas per parą ir septynias dienas per savaitę, ar šios paslaugos bus teikiamos tik darbo valandomis?

Priklausomai nuo norimo prieinamumo ir biuro įrangos (ar įmanoma, pavyzdžiui, dirbti namuose?) gali būti naudinga dirbti pagal budėjimo ar planinį tvarkaraštį.

Galima planuoti ir iniciatyviąsias, ir reagavimo paslaugas teikti darbo valandomis. Po darbo bus teikiamos tik ribotos paslaugos, pavyzdžiui, budintis darbuotojas jas teiks tik didelių nelaimių ir incidentų atveju.

Taip pat galima siekti tarptautinio bendradarbiavimo su kitomis CSIRT. Jau esama sėkmingo bendradarbiavimo pavyzdžių: *Following the Sun*. Pavyzdžiui, Europos ir Amerikos grupių bendradarbiavimas pasirodė naudingas ir yra geras būdas dalytis viena kitos pajėgumais. Štai bendrovės „Sun Microsystems“ CSIRT grupė, turinti daug filialų įvairiose laiko juostose visame pasaulyje (tačiau visi yra tos pačios CSIRT grupės nariai), teikia paslaugas 24 valandas per parą 7 dienas per savaitę: visame pasaulyje esančios grupės savo pareigas nuolat vykdo pamainomis. Tai riboja sąnaudas, nes

grupės visada dirba įprastomis darbo valandomis ir kartu teikia paslaugas „miegančiai“ pasaulio daliai.

Labai naudinga ypač nuodugniai išanalizuoti, ar klientams reikia „24x7“ paslaugų. Naktimis teikiami perspėjimai ir įspėjimai neturi prasmės, jei gavėjas juos perskaito tik ryte. „Būtinas“ ir „pageidaujamas“ paslaugas nelengva atskirti, tačiau darbuotojų ir reikiamos infrastruktūros kiekis ypač priklauso nuo darbo valandų, ir tai turi didžiausią poveikį išlaidų modeliui.

6..2 Pajamų modelis

Žinant išlaidas, kitame žingsnyje naudinga pagalvoti apie galimus pajamų modelius: kaip galima finansuoti planuojamas paslaugas. Vertinimui pateikiami keli galimi būdai.

Esamų išteklių naudojimas
Visada naudinga vertinti jau turimus kitų įmonės dalių išteklius. Gal jau yra tinkamų darbuotojų (pvz., esančiame IT skyriuje), turinčių reikiamą kvalifikaciją ir patirtį? Galbūt galima susitarti su vadovybe, kad pradiniam etapui leistų juos įdarbinti CSIRT antraeilėse pareigose arba jie galėtų padėti grupei specialiais atvejais.

Nario mokestis
Kita galimybė yra parduoti savo paslaugas aptarnaujamiems subjektams, nustačius metinį/ketvirtinį nario mokestį. Papildomos paslaugos galėtų būti apmokamos už konkrečius atvejus, pavyzdžiui, konsultavimo paslaugas ar saugumo auditus.

Kitas galimas būdas: paslaugos (vidaus) aptarnaujamiems subjektams teikiamos nemokamai, tačiau už išorės klientams suteikiamas paslaugas reikia mokėti. Kita mintis – informacinius biuletenius skelbti viešoje tinklavietėje, o skiltyje „Tik nariams“ talpinti specialią, išsamesnę arba individualią informaciją.

Praktiškai įrodyta, kad „Įmoka už CSIRT paslaugą“ naudojama ribotai, kad būtų gaunama pakankamai lėšų, ypač pradiniame etape. Yra, pavyzdžiui, nustatytos pagrindinės grupės ir įrangos išlaidos, kurias reikia padengti iš anksto. Šių išlaidų finansavimas parduodant CSIRT paslaugas yra sunkus ir reikalauja labai išsamios finansinės analizės, siekiant rasti „rentabilumo slenkstį“.

Subsidijavimas
Kita galimybė, kurią būtų verta apsvarstyti, – tai prašyti vyriausybės ar vyriausybinės institucijos subsidijuoti projektą, kadangi dabar dauguma šalių turi IT saugumo projektams skirtus fondus. Kreipimasis į Vidaus reikalų ministeriją būtų gera pradžia.

Žinoma, galima derinti kelis pajamų modelius.

Organizacinės struktūros apibrėžimas

Tinkama CSIRT organizacinė struktūra labai priklauso nuo pagrindinės organizacijos struktūros ir aptarnaujamų subjektų. Ji taip pat priklauso nuo patyrusių specialistų prieinamumo, norint juos pasamdyti nuolatinai ar specialiems atvejams.

Tipinėje CSIRT nustatomi šie vaidmenys:

Bendrasis
- Generalinis direktorius

Darbuotojai
- Biuro vadovas
- Buhalteris
- Patarėjas ryšių klausimais
- Patarėjas teisiniais klausimais

Techninė komanda veiklai
- Techninės komandos vadovas
- Techniniai CSIRT specialistai, teikiantys grupės paslaugas
- Tyrėjai

Išoriniai patarėjai
- Samdomi, kai reikia

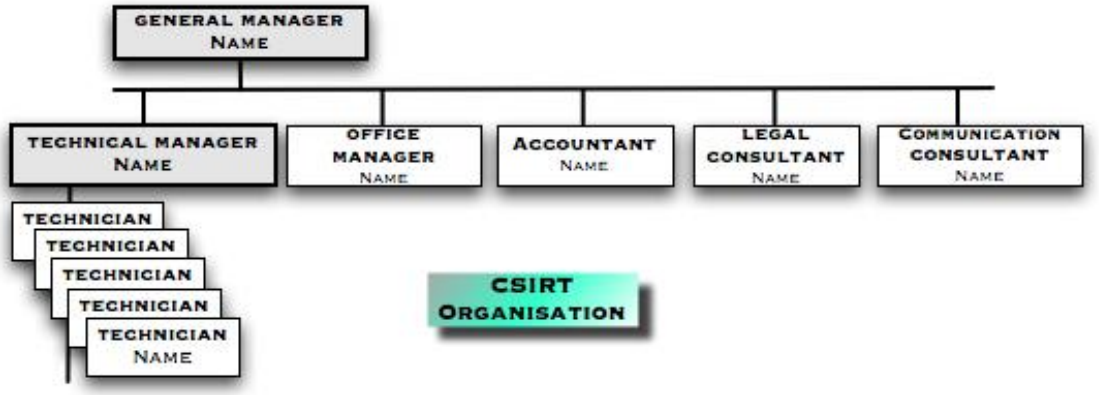
Labai naudinga grupėje turėti teisės specialistą, ypač pradiniame CSIRT veiklos etape. Tai padidins išlaidas, tačiau galiausiai sutaupys laiko ir padės išvengti teisinių rūpesčių.

Priklausomai nuo aptarnaujamų subjektų patirties įvairovės, taip pat kai CSIRT skiriamas didelis žiniasklaidos dėmesys, pasirodė, kad labai naudinga komandoje turėti ir ryšių specialistą. Šie specialistai gali sutelkti dėmesį į sunkesnių techninių klausimų perteikimą taip, kad jie būtų suprantamesni aptarnaujamiems subjektams ir žiniasklaidos partneriams. Ryšių specialistas techniniams darbuotojams taip pat pateiks aptarnaujamų subjektų atsiliepimus, taigi tarp šių dviejų grupių jis gali veikti kaip „vertėjas“ ir „bendravimo palengvintojas“.

Toliau pateikiami keli veikiančių CSIRT grupių organizacinių modelių pavyzdžiai.

6..1 Nepriklausomos įmonės modelis

CSIRT sukurta ir veikia kaip nepriklausoma įmonė, turinti savo vadovybę ir darbuotojus.

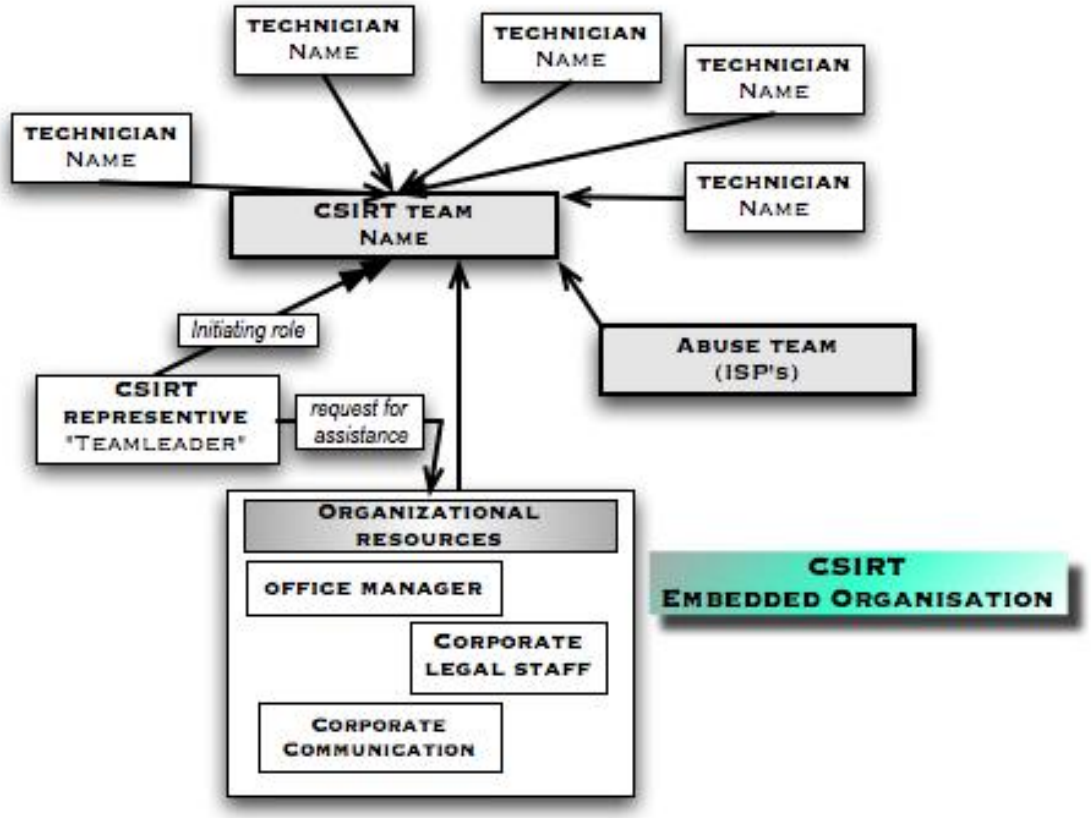


5 pav. Nepriklausomos įmonės modelis.

6..2 Integruotas modelis

Šis modelis gali būti naudingas, kai CSIRT turi būti įsteigta, pavyzdžiui, veikiančioje organizacijoje, turinčioje veikiantį IT skyrių. CSIRT grupei vadovauja komandos vadovas, atsakingas už CSIRT veiklą. Grupės vadovas parenka būtinus techninius darbuotojus, kai sprendžiami incidentai ar užsiimama CSIRT veikla. Organizacijoje jis gali paprašyti specialistų pagalbos.

Šį modelį galima pritaikyti specifinėms situacijoms, kai jos susidaro. Šiuo atveju grupė turi nustatytą darbo vietų skaičių arba priskirtą visos darbo dienos ekvivalentą (FTE). Pavyzdžiui, veikla ISP Kovos su piktnaudžiavimu skyriuje tikrai yra darbas visą darbo dieną vienam ar (daugeliu atveju) daugiau nei vienam FTE.

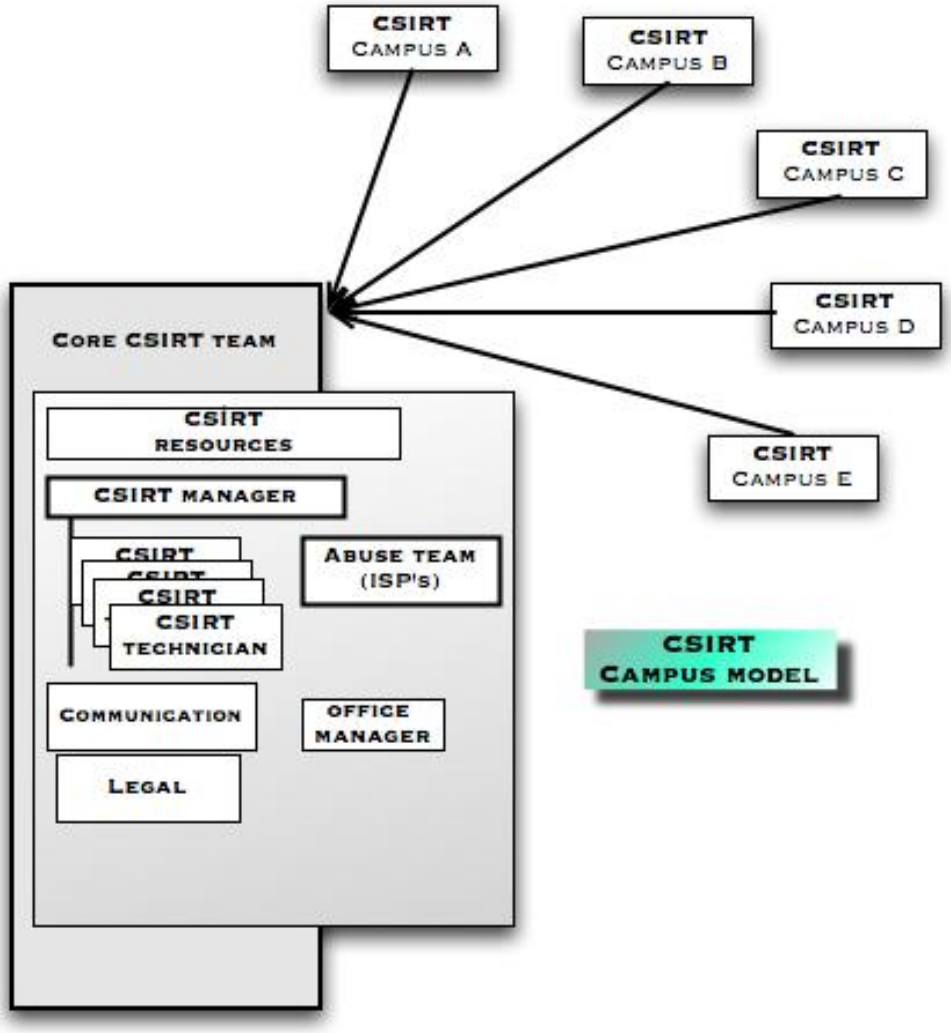


6 pav. Organizacijoje integruotas modelis.

6..3 Švietimo įstaigos teritorijos modelis

Švietimo įstaigos teritorijos modelis, kaip sako pavadinimas, daugiausiai pritaikytas akademinėms ir mokslinių tyrimų CSIRT grupėms. Dauguma akademinių ir mokslinių tyrimų organizacijų susideda iš įvairių universitetų ir jų teritorijų infrastruktūrų įvairiose vietose, išsklaidytų regione arba ir visoje šalyje (pvz., Nacionalinis tyrimų ir švietimo tinklas (NREN)). Paprastai šios organizacijos priklauso viena nuo kitos ir dažnai valdo savo CSIRT. Dažniausiai šias CSIRT globoja „motininė“ arba pagrindinė CSIRT. Pagrindinė CSIRT derina veiksmus ir yra atskira informacijos teikimo išorėn vieta. Daugeliu atveju pagrindinė CSIRT taip pat teikia pagrindines CSIRT paslaugas, taip pat atitinkamoms švietimo įstaigų teritorijų CSIRT platina informaciją apie incidentus.

Kai kurios CSIRT savo pagrindines paslaugas perduoda kitoms švietimo įstaigos teritorijos grupėms, o tai sumažina pridėtines pagrindinės CSIRT išlaidas.



7 pav. Švietimo įstaigos teritorijos modelis.

6..4 Savanoriškos veiklos modelis

Šis organizacinis modelis apibūdina grupę žmonių (specialistų), kurie susijungia, kad savanoriškai patartų ir padėtų vienas kitam (ir kitiems). Tai laisvai pritaikoma bendruomenė, labai priklausanti nuo dalyvių motyvacijos.

Šį modelį, pavyzdžiui, priėmė WARP (įspėjimų, patarimų ir pranešimų skleidimo punktų) bendruomenė[13].

Tinkamų darbuotojų samdymas

Nusprendus, kokios paslaugos ir kokio lygio pagalba bus teikiamos bei pasirinkus organizacinį modelį, kitas žingsnis – darbui rasti tinkamą kiekį kvalifikuotų žmonių.

Beveik neįmanoma pateikti tikslių skaičių apie reikiamą techninio personalo kiekį šiuo požiūriu, tačiau toliau pateikti pagrindiniai dydžiai pasitvirtino kaip geras pasirinkimas:

- Norint teikti dvi pagrindines – informacinių biuletenių ir incidentų valdymo – paslaugas: mažiausiai **4** FTE.
- Universalioms CSIRT paslaugoms darbo valandomis teikti ir sistemai prižiūrėti: mažiausiai **6-8** FTE.
- Visiškai sukomplektuota „24x7“ pamaina (2 pamainos nedarbo valandomis): mažiausiai apie **12** FTE.

Šie skaičiai taip pat apima neatėjimą į darbą dėl ligos, atostogų ir pan. Būtina taip pat patikrinti vietos kolektyvines darbo sutartis. Jei žmonės dirba ne darbo valandomis, gali atsirasti papildomų išlaidų: priemokų, kurias reikia mokėti.

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

Toliau pateikiama trumpa CSIRT techninių specialistų pagrindinių gebėjimų apžvalga.

Bendrojo techninio personalo darbo gebėjimų apibūdinimas

Asmeniniai gebėjimai

- Lankstus, kūrybingas ir palaikantis gerą komandos dvasią
- Geri analitiniai įgūdžiai
- Gebėjimas sunkius techninius dalykus paaiškinti paprastai
- Gera konfidencialumo nuojauta ir darbas laikantis procedūros
- Geri organizaciniai gebėjimai
- Atsparus stresams
- Tvirti kalbos ir rašymo įgūdžiai
- Atviras ir norintis mokytis

Techniniai gebėjimai

- Plačios žinios apie internetines technologijas ir protokolus
- „Linux“ ir „Unix“ sistemų išmanymas (priklausomai nuo aptarnaujamų subjektų įrangos)
- „Windows“ sistemų išmanymas (priklausomai nuo aptarnaujamų subjektų įrangos)
- Tinklų infrastruktūros įrangos išmanymas (maršruto parinktuvai, šakotuvai, sričių vardų (DNS), įgaliotasis (*Proxy*) serveriai, paštas ir kt.)
- Internetinių programų išmanymas (SMTP, HTTP, FTP protokolai, telnetas, SSH protokolas ir kt.)
- Saugos grėsmių išmanymas (DdoS atakos, duomenų vogimas, sugadinimas, šnipinėjimas ir kt.).
- Mokėjimas vertinti riziką ir vykdyti tai praktiškai

Papildomi gebėjimai

- Pasirengimas dirbti „24x7“ režimu ar budėti (priklausomai nuo paslaugos modelio)
- Ilgiausias kelionės nuotolis (tuo atveju, kai reikia neatidėliotinos pagalbos biure; ilgiausias kelionės laikas)
- Išsilavinimo lygis
- Darbo patirtis IT saugumo srityje

Išgalvota CSIRT (4 žingsnis)

Verslo plano sudarymas

Finansavimo modelis

Kadangi įmonė 24 valandas per parą ir 7 dienas per savaitę užsiima el. verslu ir turi tokiu pačiu metu veikiantį IT skyrių, nuspręsta, kad darbo valandomis bus teikiamos visos paslaugos, o pasibaigus darbo dienai – budinčiojo. Paslaugos aptarnaujamiems subjektams bus teikiamos nemokamai, tačiau galimybė paslaugas teikti išoriniams klientams bus apsvarstyta bandomojo ir vertinimo etapo metu.

Pajamų modelis

Pradiniame ir bandomajame etape CSIRT grupę finansuos pagrindinė įmonė. Bandomojo ir vertinimo etapo metu bus apsvarstyta papildomo finansavimo galimybė, taip pat paslaugų teikimo išorės klientams galimybė.

Organizacinis modelis
Pagrindinė organizacija yra maža įmonė, todėl pasirenkamas integruotasis modelis.
Darbo valandomis trys darbuotojai teiks pagrindines paslaugas (saugumo biuletenių platinimo ir incidentų valdymo/koordinavimo).

Įmonės IT skyriuje jau dirba tinkamos kvalifikacijos žmonės. Su šiuo skyriumi sudaromas susitarimas, kad, prireikus, CSIRT gali prašyti pagalbos tam tikrais atvejais. Be to, galima naudotis antrąja budinčių specialistų linija.
Tai bus pagrindinė CSIRT grupė, sudaryta iš keturių visą darbo dieną dirbančių narių ir penkių papildomų narių. Vienas iš jų visuomet budi.

Darbuotojai
CSIRT grupės vadovas turi kvalifikaciją apsaugos ir 1 bei 2 lygio pagalbos teikimo srityje, taip pat dirbo funkcinio atsparumo krizių valdymo veiklos srityje. Kiti trys grupės nariai yra saugos specialistai. Pusę darbo dienos dirbantys CSIRT grupės nariai iš IT skyriaus yra įmonės infrastruktūros dalies specialistai.

Biuro naudojimas ir įranga

Įranga ir biuro erdvės naudojimas bei fizinė apsauga yra labai plačios temos, todėl šiame dokumente negalima pateikti išsamaus aprašymo. Šis skyrius skirtas trumpai apžvelgti šią sritį.

Daugiau informacijos apie fizinę apsaugą galima rasti:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

„Pastato tvirtinimas“
Kadangi CSIRT dažniausiai tvarko labai slaptą informaciją, naudinga leisti grupei praktiškai kontroliuoti fizinį biuro saugumą. Tai labai priklauso nuo turimų patalpų ir infrastruktūros bei pagrindinės įmonės informacijos saugumo politikos.

Pavyzdžiui, vyriausybės dirba su klasifikavimo schemomis ir turi griežtą požiūrį į tai, kaip tvarkyti konfidencialią informaciją. Savo įmonėje ar institucijoje pasiteiraukite apie vietos taisykles ir politiką.

Dažniausiai nauja CSIRT turi bendradarbiauti su savo pagrindine organizacija, kad sužinotų vietos taisykles, politiką ir kitus teisinius aspektus.

Išsamus visos įrangos ir apsaugos priemonių, kurių reikės, aprašymas neįeina į šio dokumento taikymo sritį. Tačiau toliau rasite trumpą pagrindinių priemonių, skirtų jūsų CSIRT, sąrašą.

Bendrosios pastatui taikomos taisyklės
- Kontroliuokite įėjimą į pastatą
- Pasirūpinkite, kad bent į CSIRT biurą galėtų įeiti tik grupės darbuotojai.
- Biurus ir įėjimus stebėkite kameromis.
- Konfidencialią informaciją saugokite užrakinamoje spintelėje arba seife.
- Naudokite saugias IT sistemas.

Bendrosios IT įrangai taikomos taisyklės
- Naudokite įrangą, kuria moka naudotis darbuotojai
- Sutvirtinkite visas sistemas
- Pataisykite ir atnaujinkite visas sistemas, prieš prijungdami jas prie interneto.
- Naudokite saugumo programinę įrangą (ugniasienes, įvairias antivirusines, kovos su šnipinėjimu programas, ir kt.)

Ryšių kanalų aptarnavimas
- Vieša tinklavietė
- Uždara tinklavietės narių sritis
- Elektroniniai blankai, skirti pranešti apie incidentus
- El. paštas (PGP / GPG / S/MIME palaikymas)
- Adresatų sąrašo programa
- Aptarnaujamiems subjektams skirkite specialų telefono numerį:
    - skambinti,
    - siųsti faksu,
    - tekstinėms žinutėms (SMS) rašyti.

Įrašų sekimo sistema (-os)
- Kontaktinių duomenų bazė su grupės narių, kitų grupių ir pan. duomenimis
- CRM priemonės
- Incidentų valdymo paraiškų sistema

Nuo pat pradžių taikykite „įmonės stilių“
- Standartiniam el. laiško ir informacinio biuletenio maketui
- „Senamadiškiems“ popieriniams laiškams
- Mėnesinėms arba metinėms ataskaitoms
- Pranešimų apie incidentus blankams

Kiti aspektai
- Numatyti ryšį papildomu kanalu (*out-of-band*) užpuolimų atveju
- Numatyti interneto jungiamumo rezervavimą

Daugiau informacijos apie konkrečias CSIRT priemones rasite 8.5 skyriuje „CSIRT naudojamos priemonės“.

Informacijos apsaugos politikos kūrimas

Priklausomai nuo CSIRT rūšies, turėsite laikytis pritaikytos informacijos apsaugos politikos. Ši politika ne tik apibūdina norimą darbinių ir administracinių procesų bei procedūrų statusą, bet ir turi atitikti įstatymus bei standartus, ypač susijusius su CSIRT atsakomybe. CSIRT dažniausiai saisto nacionalinė teisė ir reglamentai, kurie dažnai yra įgyvendinami Europos teisės aktų (paprastai direktyvų) ir kitų tarptautinių susitarimų kontekste. Standartai nebūtinai yra privalomi tiesiogiai, tačiau jų laikytis gali įpareigoti ar rekomenduoti įstatymai ir teisės aktai.

Toliau pateikiamas trumpas galimų įstatymų ir politikos sąrašas

Šalies
- Įvairūs informacinių technologijų, telekomunikacijų, žiniasklaidos įstatymai
- Duomenų ir privatumo apsaugos įstatymai
- Duomenų išsaugojimo reglamentai ir kiti teisės aktai
- Finansų, apskaitos ir įmonių valdymo teisės aktai
- Bendrovių ir IT valdymo elgesio kodeksai

Europos
- Direktyva dėl elektroninių parašų (1999/93/EB)
- Direktyvos dėl duomenų apsaugos (1995/46/EB) ir elektroninių ryšių privatumo (2002/58/EB)
- Direktyvos dėl elektroninių ryšių tinklų ir paslaugų (2002/19/EB-2002/22/EB)
- Direktyvos dėl bendrovių teisės (pvz., 8-ta bendrovių teisės direktyva)

Tarptautiniai
- Bazelio komiteto Naujojo kapitalo susitarimas (*Basel* II) (ypač dėl veiklos rizikos valdymo).
- Europos Tarybos konvencija dėl elektroninių nusikaltimų
- Europos Tarybos konvencija dėl žmogaus teisių (8 straipsnis dėl privatumo)
- Tarptautiniai apskaitos standartai (IAS; iš dalies jie įpareigoja IT kontrolę)

Standartai
- Britanijos standartai BS 7799 (informacijos apsauga)
- Tarptautiniai standartai ISO2700x (informacijos apsaugos valdymo sistemos)
- Vokietijos *IT-Grundschutzbuch*, Prancūzijos EBIOS ir kitų šalių standartai

Norėdami nustatyti, ar jūsų CSIRT veikia pagal nacionalinius ir tarptautinius teisės aktus, pasitarkite su savo patarėju teisės klausimais.

Jūsų informacijos tvarkymo politika turi atsakyti į šiuos svarbiausius klausimus:

- Kaip „žymima“ arba „klasifikuojama“ gauta informacija?
- Kaip informacija tvarkoma, ypač atsižvelgiant į jos išskirtinumą?
- Kokios informacijos atskleidimo aplinkybės pasirenkamos, ypač kai su incidentu susijusi informacija perduodama kitoms grupėms ar į kitas tinklavietes.

- Ar yra kokių nors teisinių aplinkybių, į kurias reikia atsižvelgti tvarkant informaciją?
- Ar laikotės kokios nors politikos dėl slaptaraščio naudojimo, siekiant apsaugoti archyvų ir (arba) duomenų perdavimo, ypač el. paštu, išskirtinumą ir vientisumą?
- Ar į šią politiką įeina galimos teisinės ribos aplinkybės, tokios kaip viešojo rakto depozitaras (*key escrow*) arba šifravimo taikymas teisinių bylų atveju.

Išgalvota CSIRT (5 žingsnis)
Biuro įranga ir vieta Atsižvelgiant į tai, kad pagrindinėje įmonėje jau yra taikoma pakankama fizinė apsauga, ji taip pat apima ir naują CSIRT. Yra numatytas vadinamasis „pasitarimų kambarys“, skirtas veiksmams derinti ekstremalių situacijų atveju. Nupirktas seifas, skirtas koduotai medžiagai ir slaptiems dokumentams laikyti. Buvo įsteigta atskira telefono linija, įskaitant komutatorių, kad darbo valandomis būtų palengvintas ryšys specialia telefono linija, ir „budintis“ mobilusis telefonas, turintis tą patį numerį bei skirtas skambinti po darbo valandų. Be to, galima naudoti esamą įrangą ir įmonės tinklavietę su CSIRT susijusiai informacijai skelbti. Įdiegtas ir prižiūrimas adresatų sąrašas, turintis apribotą dalį bendravimui su grupės nariais ir kitomis grupėmis. Visi personalo narių kontaktiniai duomenys laikomi duomenų bazėje, spausdinta medžiaga – seife. **Reguliavimas** Kadangi CSIRT yra integruota į įmonę, turinčią informacijos apsaugos politiką, atitinkama grupės politika buvo suformuota padedant įmonės patarėjui teisės klausimais.

Bendradarbiavimo su kitomis CSIRT galimybių ir galimų nacionalinių iniciatyvų ieškojimas

Šiame dokumente jau kelis kartus minėjome, jog yra kitos CSIRT iniciatyvos ir kad joms būtina bendradarbiauti. Labai naudinga susisiekti su kitomis CSIRT kaip galima anksčiau, kad užmegztumėte reikiamą ryšį su CSIRT bendruomene. Paprastai kitos CSIRT yra labai atviros ir padeda naujai sukurtoms grupėms pradėti veiklą.

Labai naudinga pradėti nuo ENISA „CERT veiklos Europoje apžvalgos“[14] ieškant kitų šalies CSIRT grupių arba norint pradėti CSIRT bendradarbiavimo veiklą.

Norėdami rasti tinkamą CSIRT informacijos šaltinį, pagalbos kreipkitės į ENISA CSIRT ekspertus adresu

CERT-Relations@enisa.europa.eu

[14] ENISA „Apžvalga“: http://www.enisa.europa.eu/cert_inventory/

Toliau apžvelgiama CSIRT bendruomenės veikla. Daugiau informacijos ir platesnį aprašymą rasite „Apžvalgoje“.

Europos CSIRT iniciatyva

TF-CSIRT[15]
TF-CSIRT darbo grupė (*Task Force*) skatina Europos tinklų ir informacijos saugumo incidentų reagavimo grupių (CSIRT) bendradarbiavimą. Šios darbo grupės pagrindiniai tikslai – organizuoti dalijimosi patirtimi ir žiniomis forumą, pradėti teikti bandomąsias paslaugas Europos CSIRT bendruomenei ir padėti steigti naujas CSIRT.

Pagrindiniai darbo grupės tikslai:
- Organizuoti dalijimosi patirtimi ir žiniomis forumą
- Europos CSIRT bendruomenei pradėti teikti bandomąsias paslaugas
- Skatinti taikyti bendrus saugumo incidentų reagavimo standartus ir procedūras
- Padėti steigti naujas CSIRT grupes ir mokyti jų darbuotojus.
- TF-CSIRT veikla sutelkta Europoje ir aplinkinėse šalyse, laikantis 2004 m. rugsėjo 15 d. TERENA techninio komiteto priimtų darbo tvarkos taisyklių.

Visuotinė CSIRT iniciatyva

FIRST[16]
Incidentų reagavimo ir apsaugos grupių forumas (FIRST) yra svarbiausia organizacija, pripažinta geriausia pasaulyje reagavimo į incidentus srityje. Narystė FIRST įgalina incidentų reagavimo grupes veiksmingiau – reaktyviai, taip pat iniciatyviai, – reaguoti į saugumo incidentus.

FIRST suburia įvairias vyriausybinių, komercinių bei švietimo organizacijų tinklų ir informacijos saugumo incidentų reagavimo grupes. FIRST tikslas – stiprinti bendradarbiavimą ir koordinavimą incidentų prevencijos srityje, skatinti greitą reagavimą į incidentus bei remti narių ir plačiosios bendruomenės dalijimąsi informacija.

Be šio pasitikėjimo tinklo, kurį FIRST sudaro pasaulinėje incidentų reagavimo bendruomenėje, ši organizacija taip pat teikia pridėtinės vertės paslaugas.

Išgalvota CSIRT (6 žingsnis)
Bendradarbiavimo galimybių ieškojimas Naudojantis ENISA apžvalga, greitai rastos kelios CSIRT, su kuriomis susisiekta. Surengtas neseniai pasamdyto grupės vadovo susitikimas su viena iš jų. Jis susipažino su nacionalinės CSIRT veikla ir dalyvavo susirinkime. Šis susirinkimas buvo itin naudingas, nes jame pateikta darbo metodų pavyzdžių, sulaukta kelių kitų grupių paramos.

[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 Verslo plano rėmimas

Jau žengėme šiuos žingsnius:

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.
2. Nustatėme, kokiam sektoriui nauja grupė teiks savo paslaugas.
3. Aptarėme paslaugas, kurias CSIRT gali teikti savo aptarnaujamiems subjektams.
4. Išanalizavome aplinką ir aptarnaujamus subjektus.
5. Apibrėžėme veiklą.
6. Kūrėme verslo planą:
    a. apibrėžėme finansinį modelį;
    b. apibrėžėme organizacinę struktūrą;
    c. pradėjome samdyti darbuotojus;
    d. panaudojome biurą ir aprūpinome jį įranga;
    e. sukūrėme informacijos apsaugos politiką;
    f. radome partnerių bendradarbiauti.

>> Kitas žingsnis – pasinaudojus pirmiau pateiktais patarimais sudaryti veiklos projekto planą ir pradėti!

Norint apibrėžti savo veiklos projektą, pirmiausia naudinga sukurti projekto ekonominį modelį. Šis ekonominis modelis bus naudojamas kaip veiklos projekto plano pagrindas, taip pat bus naudingas kreipiantis į vadovybę dėl paramos ir gaunant biudžeto ar kitų išteklių.

Pasirodė naudinga nuolat teikti pranešimus vadovybei, siekiant palaikyti gerą informuotumą apie IT saugos problemas, ir tuo būdu nuolat gauti paramos savo CSIRT.

Ekonominis modelis pradedamas kurti problemas ir galimybes išanalizuojant pagal 5.3 skyriuje „Aptarnaujamų subjektų analizė“ aprašytą analizės modelį, ir ieškant glaudžių kontaktų su galimais aptarnautinais subjektais.

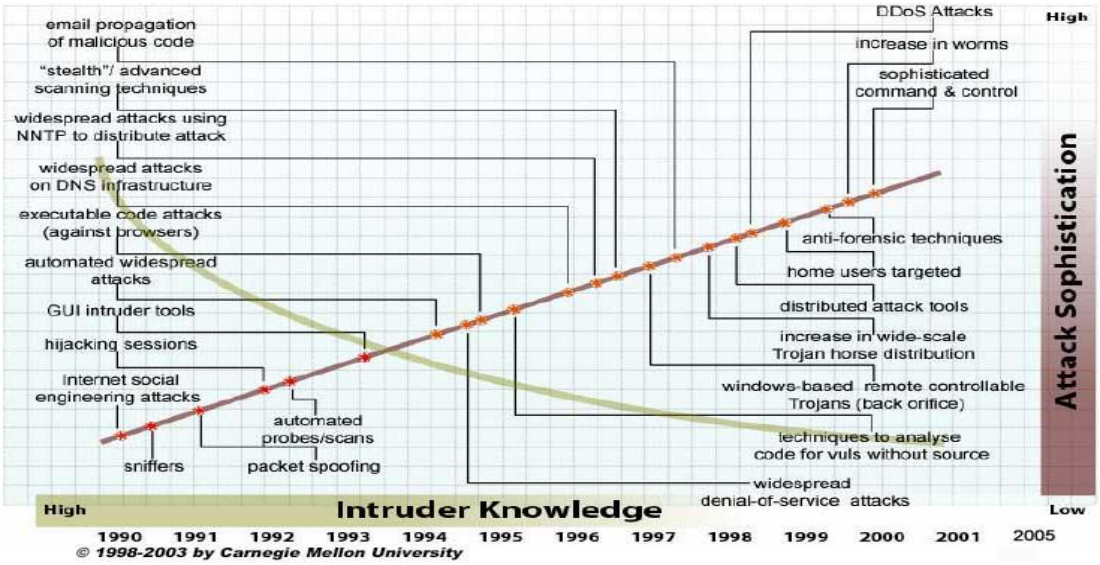
Kaip pasakyta anksčiau, pradedant kurti CSIRT yra daug apie ką pagalvoti. Geriausia pirmiau pateiktą medžiagą pritaikyti prie CSIRT poreikių, kai jie paaiškėja.

Teikiant ataskaitą vadovybei, labai naudinga savo ekonominį modelį papildyti naujausiais duomenimis, panaudojant naujausius straipsnius iš laikraščių ar interneto, ir paaiškinti, kodėl CSIRT paslauga ir vidinis incidentų koordinavimas yra ypač svarbūs įmonės turto saugumui. Be to, būtina išaiškinti, kad tik nuolatinė parama IT apsaugos srityje lemia įmonės, ypač nuo IT priklausančios bendrovės ar institucijos, tvarumą.

(Garsus Bruce'o Schneier'io posakis šiuo atveju labai tinka: *„Security is not a product but a process[17]!“ (Apsauga – ne produktas, o procesas!))*

Žinoma priemonė saugumo problemoms iliustruoti yra šis CERT/CC pateiktas grafikas:

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



8 pav. Įsibrovėlio žinios palyginti su užpuolimo sudėtingumu (šaltinis: CERT-CC[18]).

Jis parodo IT saugumo tendencijas, ypač vis sudėtingesniems užpuolimams vykdyti būtinų įgūdžių mažėjimą.

Kitas minėtinas aspektas – nuolat mažėjantis laiko tarpas tarp programinės įrangos atnaujinimo dėl pažeidžiamumo ir jos puolimo pradžios:

Pataisa -> Pažeidžiamumas		**Plitimo greitis**	
„Nimda“:	11 mėnesių	„Raudonasis kodas“:	Dienos
„Slammer“:	6 mėnesiai	„Nimda“:	Valandos
„Nachi“:	5 mėnesiai	„Slammer“:	Minutės
„Blaster“:	3 savaitės		
„Witty“:	1 diena (!)		

Surinkti incidentų duomenys, galimi patobulinimai ir įgyta patirtis taip pat gerai tinka rengiant pristatymą.

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

Veiklos planų apibūdinimas ir vadovybės paskatinimas

Vadovybei skirtas pristatymas, įskaitant pačios CSIRT reklamą, dar nėra ekonominis modelis, tačiau, atitinkamai jį parengus, daugeliu atveju jis padeda sulaukti vadovybės paramos CSIRT. Kita vertus, ekonominio modelio nereikia laikyti tik vadybos pratybomis. Jis taip pat turi būti naudojamas bendrauti su grupe ir aptarnaujamais subjektais. Terminas „ekonominis modelis“ gali skambėti labai komerciškai ir toli gražu neatitikti kasdienės CSIRT veiklos, tačiau jis padeda sutelkti dėmesį ir pastangas steigiant CSIRT.

Atsakymai į toliau pateiktus klausimus gali būti naudojami geram projekto ekonominiam modeliui sukurti (pateikti pavyzdžiai yra hipotetiniai ir naudojami tik paaiškinti. „Tikri“ atsakymai labai priklauso nuo „tikrų“ aplinkybių).

- Kokia problema?
- Ko norite pasiekti savo aptarnaujamų subjektų atžvilgiu?
- Kas bus, jei nieko nedarysite?
- Kas bus, jei imsitės veiksmų?
- Kiek tai kainuos?
- Kokia bus nauda?
- Kada pradėsite veiklą ir kada ji baigsis?

Kokia problema?
Daugeliu atveju mintis įsteigti CSIRT kyla, kai IT saugumas tampa gyvybiškai svarbia įmonės ar įstaigos pagrindinės veiklos dalimi ir kai IT saugumo pažeidimai pradeda kelti pavojų įmonei, todėl saugumo rizikos mažinimas tampa įprastine įmonės veikla.

Dauguma įmonių ar institucijų turi nuolatinius pagalbos skyrius ar tarnybas, tačiau daugeliu atveju saugumo pažeidimai tvarkomi nepakankamai ir ne taip struktūrizuotai, kaip turėtų būti. Dažniausiai darbui saugumo pažeidimų srityje būtini specialūs įgūdžiai ir dėmesys. Taikyti labiau susistemintą metodą taip pat naudinga: tai mažina veiklos riziką ir žalą įmonei.

Daugeliu atveju problema yra ta, kad nederinami veiksmai ir turimos žinios nenaudojamos incidentams valdyti, o tai galėtų jiems užkirsti kelią ateityje ir apsaugoti nuo galimų finansinių nuostolių ir (arba) žalos geram institucijos vardui.

Kokių tikslų reikia pasiekti aptarnaujamų subjektų atžvilgiu?
Kaip jau sakėme, jūsų CSIRT teiks paslaugas savo aptarnaujamiems subjektams ir padės jiems spręsti IT saugos incidentus ir problemas. IT saugumo žinių lygio kėlimas ir saugumo suvokimo kultūros siekimas yra papildomi tikslai.

Ši kultūra skatina nuo pat pradžių imtis iniciatyvių ir prevencinių priemonių, taip sumažinant veiklos išlaidas.

Įmonės ar įstaigos supažindinimas su šia bendradarbiavimo ir pagalbos kultūra daugeliu atveju skatina efektyvumą apskritai.
Kas nutinka, jei nieko nedaroma?

Struktūriškai neapibrėžtas IT apsaugos valdymas gali lemti tolesnę žalą, ypač geram įstaigos vardui. Kiti padariniai gali būti finansiniai nuostoliai ir teisinės pasekmės.

Kas nutinka, jei imamasi veiksmų?
Padidinamas informuotumas apie saugumo problemų paplitimą. Tai padeda jas spręsti efektyviau ir užkerta kelią būsimiems nuostoliams.

Kiek tai kainuos?
Priklausomai nuo organizacinio modelio, išlaidas sudarys CSIRT grupės narių atlyginimai ir organizacijos, įrangos, priemonių ir programinės įrangos licencijos.

Kokia bus nauda?
Priklausomai nuo veiklos ir nuostolių praeityje, bus pasiektas procedūrų ir apsaugos praktikos skaidrumas, taip apsaugant pagrindinį įmonės turtą.

Koks laikotarpis?
Žiūrėkite 12 skyrių „Veiklos projekto planas“, kuriame pateikiamas veiklos projekto plano pavyzdys.

Veikiančių ekonominių modelių ir metodų pavyzdžiai
Štai keli CSIRT ekonominiai modeliai, kuriuos verta išnagrinėti:

- http://www.cert.org/csirts/AFI_case-study.html
  Finansinės institucijos CSIRT kūrimas: konkretaus atvejo analizė

  Šio dokumento tikslas – pasidalyti finansinės institucijos (šiame dokumente nurodomos kaip AFI) patirtimi, įgyta kuriant ir įgyvendinant saugumo problemų spendimo planą bei steigiant tinklų ir informacijos saugumo incidentų reagavimo grupę.

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Įmonės CERT POLSKA verslo ekonominio modelio apibendrinimas (skaidrių demonstracija PDF formatu)

- http://www.auscert.org.au/render.html?it=2252
  Incidentų reagavimo grupės (IRT) kūrimas dešimtajame dešimtmetyje gali būti bauginanti užduotis. Daugelis IRT kuriančių žmonių tam neturi jokios patirties. Šiame dokumente nagrinėjama, kokį vaidmenį IRT gali vaidinti bendruomenėje, ir aspektai, į kuriuos reikia atkreipti dėmesį kuriant grupę ir pradėjus veiklą. Jis gali būti naudingas veikiančioms IRT, kadangi tai gali padėti geriau suvokti tuos aspektus, į kuriuos anksčiau nebuvo kreipiamas dėmesys.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Konkretaus atvejo informacijos apsaugos srityje analizė: „Įmonės apsauga“. Autorius Roger'is Benton'as

  Šios pratybos yra draudimo bendrovės perėjimo į visos įmonės apsaugos sistemą analizė. Šių pratybų tikslas – parodyti kelią, kuriuo reikia eiti kuriant apsaugos sistemą arba pereinant į ją. Iš pradžių nesudėtinga interneto apsaugos sistema buvo vienintelis mechanizmas kontroliuoti prieigai prie įmonės duomenų. Išorinis poveikis buvo skaudus, nes nebuvo vieningos kontrolės ne interneto aplinkoje. Kiekvienas, turintis pagrindinius programavimo įgūdžius, galėjo papildyti, pakeisti ir (arba) panaikinti gamybos duomenis.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Įmonės „Marriott“ elektroninės apsaugos strategija: verslo IT bendradarbiavimas

  Remiantis bendrovės „Marriott International, Inc.“ darbuotojo Chris'o Zoladz'o patirtimi, elektroninio verslo apsauga yra procesas, o ne projektas. Tokią mintį Zoladz'as pasakė Bostone neseniai vykusioje Elektroninio saugumo konferencijoje ir parodoje, kurią rėmė bendrovė „Intermedia Group“. „Marriott“ informacijos apsaugos viceprezidentas Zoladz'as pranešimus teikia per teisės skyrių, nors jis nėra teisininkas. Jo pareigos – nustatyti, kur laikoma vertingiausia bendrovės verslo informacija ir kaip ji juda įmonės viduje bei išorėje. „Marriott“ turi atskirą įsipareigojimą teikti pagalbinę techninės infrastruktūros apsaugą, patikėtą IT apsaugos kūrėjui.

Išgalvota CSIRT (7 žingsnis)
Verslo plano rėmimas Nuspręsta rinkti faktus ir skaičius iš įmonės istorijos. Tai itin padeda atlikti statistinę IT apsaugos padėties apžvalgą. Įkūrus CSIRT ir jai veikiant, jie turi būti renkami toliau, kad statistiniai duomenis būtų nuolat aktualizuojami. Susisiekta su kitomis šalies CSIRT ir pasikalbėta apie jų ekonominius modelius. Jos padėjo – parengė skaidrių su informacija apie pastarojo meto įvykius IT apsaugos incidentų srityje ir dėl incidentų patirtas išlaidas. Šiuo išgalvotos CSIRT atveju nebuvo didelės būtinybės įtikinėti vadovybės dėl IT verslo svarbos, todėl nebuvo sunku gauti leidimą žengti pirmą žingsnį. Parengtas ekonominis modelis ir projekto planas, taip pat steigimo ir veiklos išlaidų vertinimas.

8 Veiklos ir techninių procedūrų pavyzdžiai (darbų srautas)

Jau žengėme šiuos žingsnius:

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.
2. Nustatėme, kokiam sektoriui nauja grupė teiks savo paslaugas.
3. Aptarėme paslaugas, kurias CSIRT gali teikti savo aptarnaujamiems subjektams.
4. Išanalizavome aplinką ir aptarnaujamus subjektus.
5. Apibrėžėme veiklą.
6. Sukūrėme verslo planą.
   a. Apibrėžėme finansinį modelį.
   b. Apibrėžėme organizacinę struktūrą.
   c. Pradėjome samdyti darbuotojus.
   d. Panaudojome biurą ir aprūpinome jį įranga.
   e. Sukūrėme informacijos apsaugos politiką.
   f. Ieškojome partnerių bendradarbiauti.
7. Parėmėme verslo planą.
   a. Buvo patvirtintas ekonominis modelis.
   b. Viską pritaikėme veiklos projekto planui.

>> Kitas žingsnis: pradėti CSIRT veiklą.

Aiškiai apibrėžus darbų srautus, pagerėja kokybė ir racionaliau naudojamas incidento ar pažeidžiamumo atvejui reikiamas laikas.

Kaip apibūdinta pavyzdžių lentelėse, išgalvota CSIRT teiks pagrindines paslaugas:

- Perspėjimus ir įspėjimus
- Incidentų valdymą
- Pranešimus

Šiame skyriuje pateikiami darbo srautų pavyzdžiai, apibūdinantys pagrindines CSIRT paslaugas. Šiame skyriuje taip pat aiškinama apie informacijos rinkimą iš įvairių šaltinių, jos tinkamumo bei autentiškumo tikrinimą ir perdavimą aptarnaujamiems subjektams. Ir, galiausiai, jame yra pačių pagrindinių procedūrų ir specifinių CSIRT priemonių pavyzdžių.

Aptarnaujamų subjektų programinės įrangos bazės vertinimas

Pirmiausia reikia surinkti duomenis apie jūsų aptarnaujamų subjektų naudojamas IT sistemas. Remdamasi jais, CSIRT gali vertinti priimamos informacijos tinkamumą ir filtruoti ją prieš perskirstydama, kad aptarnaujami subjektai nebūtų užliejami jiems dažniausiai nenaudinga informacija.

Geriausia pradėti paprastai, pavyzdžiui, naudoti skaičiuoklės (*excel*) darbo lapą, kaip šis:

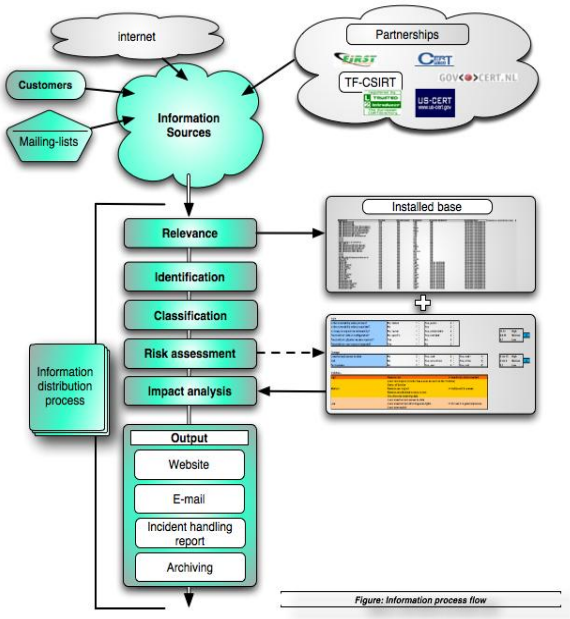
Kategorija	Pritaikymas	Programa	Versija	OS	OS versija	Aptarnauja-mas subjektas
Stalinis kompiuteris	Biuras	„Excel“	x-x-x	„Microsoft“	„XP-prof“	A
Stalinis kompiuteris	Naršyklė	IE	x-x-	„Microsoft“	„XP-prof“	A
Tinklas	Maršruto parinktuvas	CISCO	x-x-x	CISCO	x-x-x-	B
Serveris	Serveris	„Linux“	x-x-x	„L-distro“	x-x-x	B
Paslaugos	Žiniatinklio serveris	„Apache“		„Unix“	x-x-x	B

Nustačius skaičiuoklės filtro funkciją, labai lengva parinkti tinkamą programą ir pažiūrėti, koks aptarnaujamas subjektas kokią programą naudoja.

Perspėjimų, įspėjimų ir pranešimų rengimas

Visi perspėjimai, įspėjimai ir pranešimai rengiami atlikus tuos pačius darbus:

- Surinkus informaciją
- Vertinus jos tinkamumą ir šaltinį
- Atlikus rizikos vertinimą remiantis surinkta informacija
- Paskirsčius informaciją



9 pav. Informacijos apdorojimo srautas.

Kitose dalyse šis darbų srautas aiškinamas plačiau.

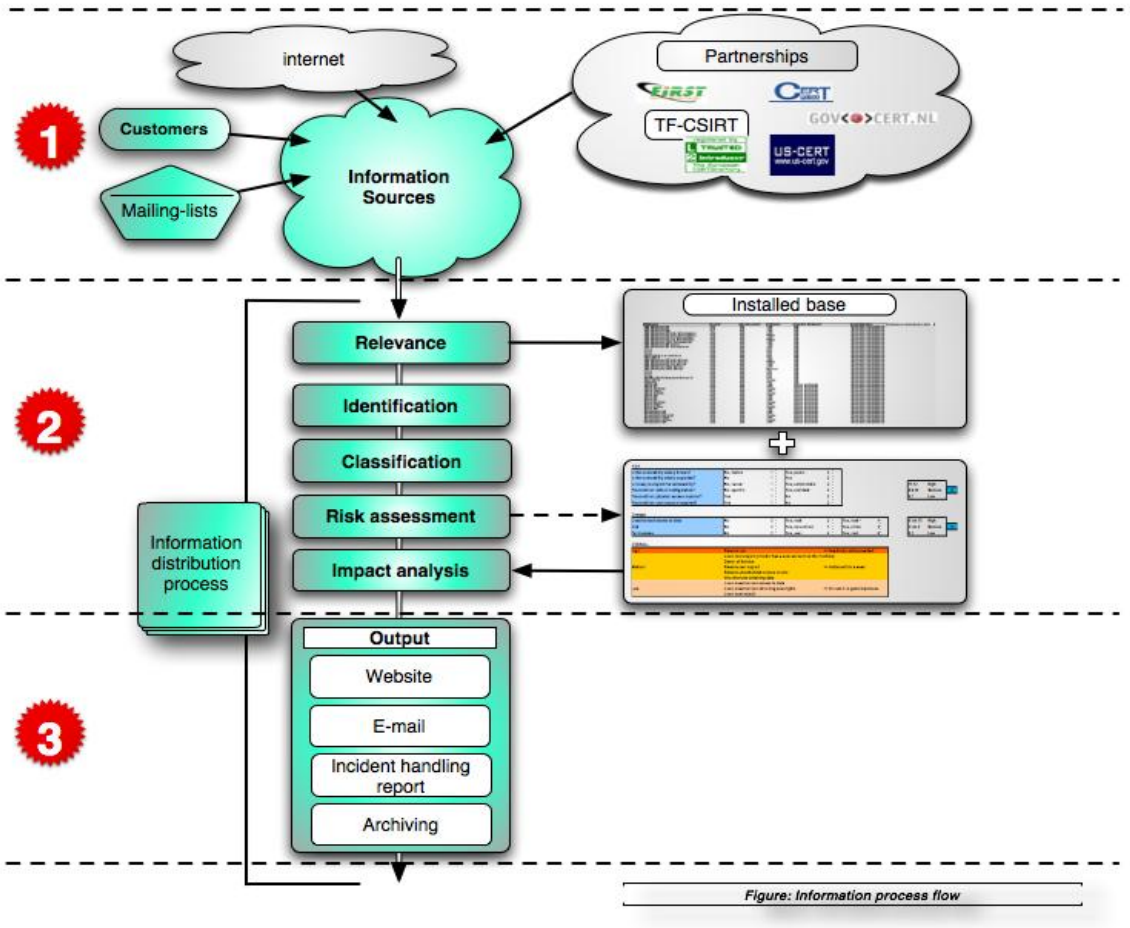


Figure: Information process flow

1 žingsnis: informacijos apie sistemų pažeidžiamumą rinkimas

Paprastai yra dviejų pagrindinių tipų informacijos šaltiniai, kurių teikiama informacija yra įnašas į paslaugas:

- Informacija apie (jūsų) IT sistemų pažeidžiamumą
- Pranešimai apie incidentus

Priklausomai nuo verslo rūšies ir IT infrastruktūros, yra daug viešųjų ir uždarų informacijos apie pažeidžiamumą šaltinių:

- Vieši ir uždari adresatų sąrašai
- Informacija apie gamintojo produkto pažeidžiamumą
- Tinklavietės
- Informacija internete („Google“ ir kt.)
- Viešosios ir privačios bendrijos, teikiančios informaciją apie pažeidžiamumą (FIRST, TF-CSIRT, CERT-CC, US-CERT, kt.)

Visa ši informacija gerina žinių apie konkrečias silpnas IT sistemos vietas lygį.

Kaip pasakyta anksčiau, internete yra daug gerų ir lengvai prieinamų šaltinių apie informacijos apsaugą. ENISA *ad-hoc* darbo grupė "CERT paslaugos" 2006-iais raštu kuria išsamesnį sąrašą, kurio tikimasi sulaukti 2006 m. pabaigoje[19].

2 žingsnis: informacijos analizė ir rizikos vertinimas

Šioje dalyje analizuojamas konkretaus pažeidžiamumo poveikis aptarnaujamų subjektų IT infrastruktūrai.

Identifikavimas
Priimama informacija apie pažeidžiamumą visada turi būti identifikuojama remiantis jos šaltiniu, ir, prieš teikiant bet kokią informaciją aptarnaujamiems subjektams, turi būti nustatyta, ar šaltinis patikimas. Kitaip žmonės gali būti melagingai įspėjami, o tai gali bereikalingai sutrikdyti verslo procesus ir galiausiai pakenkti geram CSIRT vardui.

[19] Ad-hoc darbo grupės CERT paslaugos:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Toliau pateikta procedūra yra pranešimo autentiškumo nustatymo pavyzdys:

Pranešimo autentiškumo ir jo šaltinio nustatymo procedūra

Bendrasis kontrolinis sąrašas
1. Ar šaltinis žinomas ir yra įregistruotas?
2. Ar informacija siunčiama įprastiniu kanalu?
3. Ar joje yra „keistos“ informacijos, keliančios įtarimą?
4. Paisykite savo įtarimo: jei abejojate informacija, nesiimkite veiksmų, bet vėl ją patikrinkite!

Elektroninis paštas: šaltiniai
1. Ar organizacijai žinomas šaltinio adresas, ar jis įtrauktas į šaltinių sąrašą?
2. Ar teisingas PGP parašas?
3. Jei kyla abejonių, patikrinkite visą laiško antraštę.
4. Jei abejojate, siuntėjo sričiai patikrinti naudokite komandas „nslookup“ arba „dig“ [20].

WWW: šaltiniai
1. Patikrinkite naršyklės sertifikatus, jei jungiatės prie saugomos tinklavietės (https://).
2. Patikrinkite šaltinio turinį ir galiojimą (techninį).
3. Jei kyla abejonių, nespauskite jokių saitų arba nesisiųskite jokių programų.
4. Jei kyla abejonių, naudokite komandas „lookup“ arba „dig“ domenui patikrinti ir naudokite programą „traceroute“.

Telefonas
1. Atidžiai klausykitės asmenvardžių.
2. Ar pažįstamas balsas?
3. Jei kyla abejonių, paklauskite telefono numerio ir paprašykite skambinančiojo paskambinti dar kartą.

10 pav. Informacijos identifikavimo procedūros pavyzdys.

Tinkamumas
Anksčiau pateikta įdiegtos aparatinės ir programinės įrangos apžvalga gali būti naudojama gaunamai informacijai apie pažeidžiamumą filtruoti tinkamumo atžvilgiu, turint tikslą rasti atsakymą į klausimus: „Ar aptarnaujami subjektai naudoja šią programinę įrangą?“, „Ar informacija jiems tinkama?“

Klasifikavimas
Kai kuri gaunama informacija gali būti klasifikuojama arba pažymima kaip apribota (pvz., iš kitų grupių gaunami pranešimai apie incidentus). Visa informacija turi būti tvarkoma pagal siuntėjo poreikius ir vadovaujantis savo pačių informacijos saugumo politika. Naudinga laikytis pagrindinės taisyklės: „*Neskirstykite informacijos, jei nėra aišku, ar tai yra numatyta. Jei kyla abejonių, paprašykite siuntėjo leidimo tai padaryti*“.

[20] CHIHT siūlomos tapatybės tikrinimo priemonės: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Rizikos vertinimas ir poveikio analizė
Yra keli (galimo) pažeidžiamumo rizikos ir poveikio nustatymo būdai.

Rizika apibrėžiama kaip pasinaudojimo pažeidžiamumu galimybė. Be kitų, yra keli svarbūs veiksniai:

- Ar pažeidžiamumas gerai žinomas?
- Ar pažeidžiamumas plačiai paplitęs?
- Ar lengva pasinaudoti pažeidžiamumu?
- Ar šiuo pažeidžiamumu galima pasinaudoti nuotoliniu būdu?

Visi šie klausimai padeda gerai suprasti pažeidžiamumo rimtumą.
Labai paprastas būdas rizikai apskaičiuoti yra ši formulė:

Poveikis = Rizika X galima Žala

Galima žala gali būti:

- Neteisėta prieiga prie duomenų
- Paslaugos atsisakymas (DOS)
- Leidimų įgijimas arba jų galiojimo laiko pratęsimas

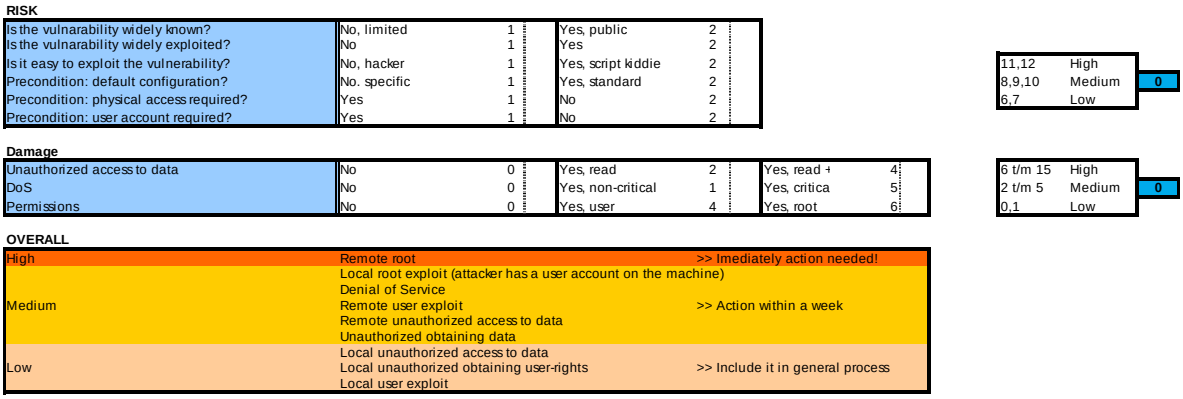
(Daugiau detalizuotų klasifikacijų pateikta šio skyriaus pabaigoje).

Atsakius į šiuos klausimus, bendras vertinimas gali būti įtrauktas į saugos biuletenį, pranešantį apie galimą riziką ir žalą. Dažnai naudojami paprasti terminai, pvz., MAŽA, VIDUTINĖ ir DIDELĖ.

Kitos, išsamesnės rizikos vertinimo schemos:

GOVCERT.NL vertinimo schema[21]

Olandijos vyriausybinė CSIRT GOVCERT.NL tobulina rizikos vertinimo lentelę, kuri buvo sukurta „Govcert.nl“ steigiamajame etape ir atnaujinama atsižvelgiant į naujausias tendencijas.



11 pav. GOVCERT.NL vertinimo schema.

EISPP bendros biuletenio formos apibūdinimas[22]

Europos informacijos apsaugos skatinimo programa (EISPP) (*European Information Security Promotion Programme*) yra projektas, Europos bendrijos bendrai finansuojamas pagal Penktąją pagrindų programą. EISPP projekto tikslas – sukurti Europos sistemą, skirtą ne tik dalytis apsaugos žiniomis, bet ir apibrėžiančią apsaugos informacijos turinį bei jos paskirstymo mažoms ir vidutinėms įmonėms (MVĮ) būdus. Europos MVĮ teikiant būtinas IT apsaugos paslaugas, jos bus skatinamos labiau pasitikėti ir naudotis elektronine komercija, lemiančia padidėjusias ir geresnes galimybes kurti naują verslą. EISPP yra Europos Komisijos vizijos Europos Sąjungoje sukurti Europos žinių tinklą pradininkas.

DAF Vokietijos biuletenio forma[23]

DAF yra Vokietijos CERT-*Verbund* iniciatyva ir pagrindinė infrastruktūros, skirtos kaupti bei keistis įvairių grupių apsaugos informaciniais biuleteniais, sudedamoji dalis. DAF yra specialiai pritaikyta Vokietijos CERT poreikiams. Standartą sukūrė ir palaiko CERT-*Bund*, DFN-CERT, PRESECURE ir *Siemens*-CERT.

[21] Pažeidžiamumo lentelė: 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 žingsnis: informacijos paskirstymas

CSIRT gali rinktis iš kelių paskirstymo būdų, priklausomai nuo aptarnaujamų subjektų pageidavimo ir jūsų ryšių strategijos.

- Tinklavietė
- El. paštas
- Pranešimai
- Archyvavimas ir tyrimas

CSIRT platinami apsaugos patarimų biuleteniai visada turi turėti tą pačią struktūrą. Tai pagerina skaitomumą, todėl skaitytojas greitai randa susijusią informaciją.

Informaciniame biuletenyje turi būti bent jau ši informacija:

Informacinio biuletenio pavadinimas ……
Nuorodos numeris …… **Pažeistos sistemos** - …… - …… **Susijusi OS ir versija** …… **Rizika** (didelė, vidutinė, maža) …… **Poveikis/galima žala** (didelė, vidutinė, maža) …… **Išoriniai ID:** (CVE, Pažeidžiamumo biuletenio ID) ……
Pažeidžiamų vietų apžvalga …… **Poveikis** …… **Sprendimas** …… **Aprašymas (išsamus)** …… **Priedėlis** ……

12 pav. Informacinio biuletenio struktūros pavyzdys.

Žiūrėkite 10 skyrių. *Praktiškai sukurkite* visiškai užbaigto apsaugos informacinio biuletenio pavyzdį.

Incidentų valdymo procesas

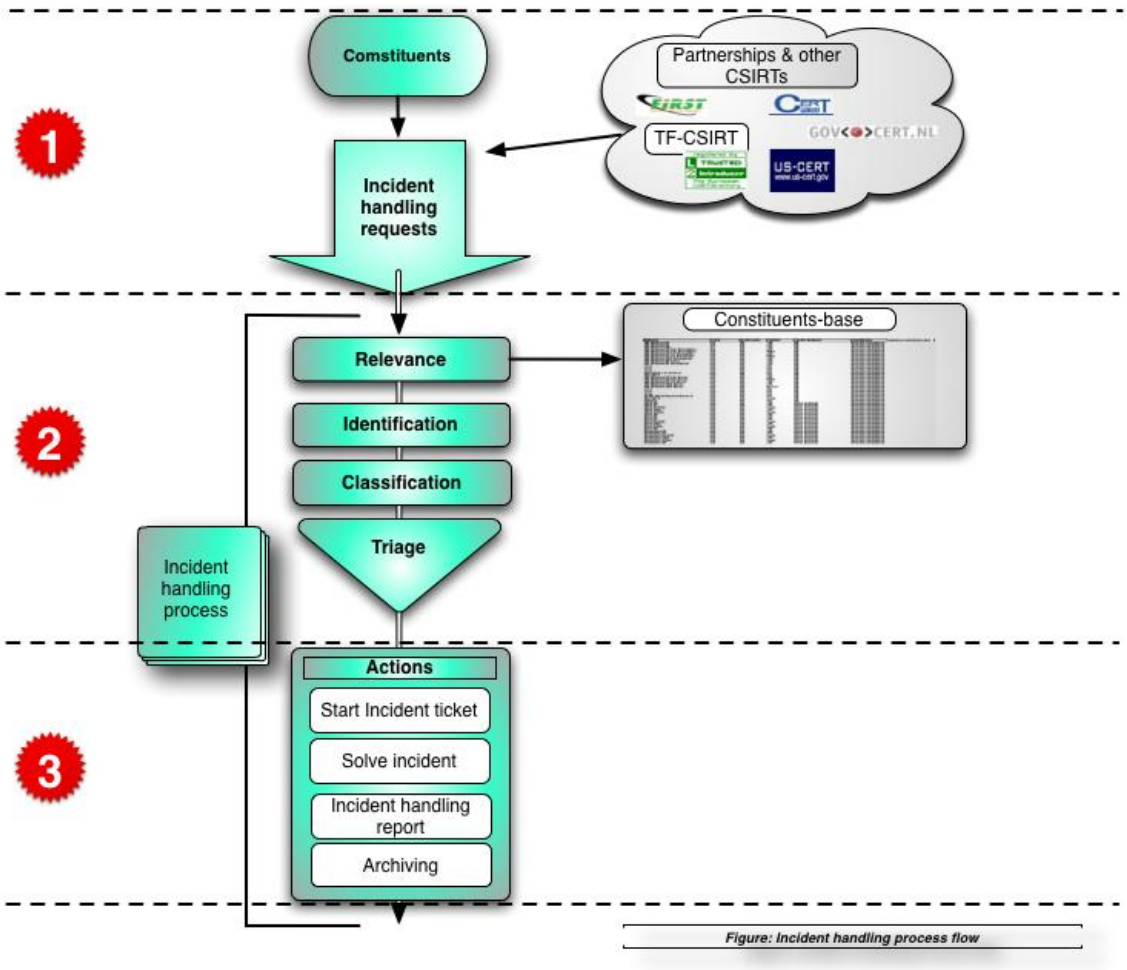
Kaip minėta šio skyriaus įvade, informacijos tvarkymo būdas valdant incidentus labai panašus į tą, kuris naudojamas renkant perspėjimus, įspėjimus ir pranešimus. Tačiau informacijos rinkimo dalis paprastai skiriasi, kadangi su incidentu susiję duomenys paprastai gaunami aptarnaujamų subjektų ar kitų grupių pranešimuose apie incidentus arba incidento valdymo metu siunčiamuose procese dalyvaujančių šalių atsiliepimuose. Dažniausiai informacija gaunama el. paštu (šifruotu); kartais reikia naudoti telefoną ar faksą.

Informaciją gaunant telefonu, naudinga tuoj pat užsirašyti visas smulkmenas arba naudojant incidentų valdymo/pranešimo apie juos programą, arba sudarant atmintinę. Būtina nedelsiant (prieš baigiantis pokalbiui telefonu) sukurti incidento numerį (jei šiam incidentui numeris dar nebuvo priskirtas) ir pasakyti jį pranešėjui telefonu (arba nurodyti po to išsiunčiamame apibendrinamajame el. laiške), nes tai bus tolesnio bendravimo nuoroda.

Toliau šioje dalyje aprašomi incidentų valdymo proceso pagrindai. Labai išsamią viso incidentų valdymo proceso analizę ir visus joje atliekamų darbų srautus bei posraučius galima rasti CERT/CC dokumentuose *„CSIRT grupių incidentų valdymo procesų nustatymas“ (Defining Incident Management processes for CSIRTs)*[24].

[24] Incidentų valdymo procesų nustatymas: http://www.cert.org/archive/pdf/04tr015.pdf.

Iš esmės, incidentų valdymui būdingas šis darbų srautas:



13 pav. Incidento proceso eiga.

1 žingsnis: pranešimo apie incidentą gavimas

Kaip minėta anksčiau, pranešimai apie incidentus CSIRT pasiekia keliais kanalais, dažniausiai el. paštu, taip pat telefonu arba faksu.

Jau sakėme, kad priimant pranešimą apie incidentą, visas smulkmenas labai naudinga užsirašyti fiksuota forma. Taip užtikrinama, kad jokia ypač svarbi informacija nebūtų praleista. Naudojant schemos pavyzdį, galima sužinoti:

PRANEŠIMO APIE INCIDENTĄ BLANKAS
Užpildykite šį blanką ir atsiųskite faksu arba el. paštu: …….. *Žvaigždute (*) pažymėtus duomenis pateikti būtina.* *Vardas, pavardė ir organizacija* 1. Vardas, pavardė*: 2. Organizacijos pavadinimas*: 3. Sektoriaus tipas: 4. Šalis*: 5. Miestas: 6. El. pašto adresas:* 7. Telefono numeris*: 8. Kita: *Pakenkti pagrindiniai kompiuteriai* 9. Pagrindinių kompiuterių skaičius: 10. Pagrindinio kompiuterio pavadinimas ir IP*: 11. Pagr. kompiuterio funkcija*: 12. Laiko juosta: 13. Aparatinė įranga: 14. Operacinė sistema: 15. Paveikta programinė įranga: 16. Paveikti failai: 17. Apsauga: 18. Pagrindinio kompiuterio pavadinimas ir IP: 19. Protokolas/prievadas *Incidentas* 20. Nuorodos numeris (Nuor. Nr.) 21. Incidento tipas: 22. Incidento pradžia: 23. Tai tebevykstantis incidentas: TAIP NE 24. Aptikimo laikas ir būdas: 25. Žinomos pažeidžiamos vietos: 26. Įtartini failai: 27. Atsakomosios priemonės: 28. Išsamus aprašymas*:

14 pav. Pranešimo apie incidentą turinys.

2 žingsnis: incidento vertinimas

Šiame etape patikrinamas nurodyto incidento autentiškumas ir tinkamumas, jis priskiriamas tam tikrai kategorijai.

Identifikavimas

Norint išvengti nebūtinų veiksmų, naudinga patikrinti, ar siuntėjas patikimas ir ar jis yra vienas iš jūsų arba kolegų CSIRT aptarnaujamų subjektų. Taikomos panašios taisyklės, kaip aprašyta 8.2 skyriuje „Perspėjimų kūrimas“

Tinkamumas

Šiame etape patikrinate, ar prašymą tirti incidentą atsiuntė CSIRT aptarnaujami subjektai, ar nurodytas incidentas apima aptarnaujamų subjektų IT sistemas. Jei netinka nė vienas iš nurodytų atvejų, pranešimas dažniausiai nukreipiamas reikiamai CISRT[25].

Klasifikavimas

Šiame etape pagalbos pirmumas nustatomas klasifikuojant pagal pažeidimo sunkumą. Išsamus incidentų (pažeidimų) klasifikavimas neįeina į šio dokumento taikymo sritį. Pradžioje naudinga taikyti CSIRT modelio klasifikaciją (Pavyzdys įmonės CSIRT grupei):

Incident Categories

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

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

15 pav. Incidento klasifikavimas (šaltinis: FIRST[26]).

[25] CHIHT siūlomos tapatybės tikrinimo priemonės: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] CSIRT modelio klasifikavimas http://www.first.org/resources/guides/csirt_case_classification.html.

Pagalbos pirmumo nustatymas

Pagalbos pirmumo nustatymas – tai sistema, kurią medicinos ar greitosios pagalbos personalas naudoja ribotiems medicininiams ištekliams normuoti, kai sužeistųjų, kuriems reikia pagalbos, skaičius viršija tai pagalbai būtinų išteklių kiekį, kad galėtų suteikti pagalbą kaip galima didesniam pacientų skaičiui[27].

CERT/CC pateikiamas apibūdinimas:

Pagalbos pirmumo nustatymas yra pagrindinė incidentų valdymo pajėgumų dalis, ypač visų įsteigtų CSIRT. Pagalbos pirmumo nustatymas yra svarbiausias kelias, norint suprasti, ką pranešė organizacija. Jis veikia kaip transporto priemonė, kuria visa informacija gabenama į atskirą informacijos teikimo vietą, leidžiančią įmonei peržvelgti vykdomą veiklą ir visapusišką visų pateiktų duomenų sąsają. Pagalbos pirmumo nustatymas leidžia atlikti pradinį gaunamo pranešimo vertinimą ir nustato jo tolesnio tvarkymo eilę. Jis taip pat pateikia vietą pradiniams dokumentavimui pradėti ir pranešimo ar prašymo duomenims įvesti, jei tai dar nebuvo padaryta aptikimo proceso metu.

Ši funkcija padeda greitai susidaryti glaustą nurodytų veiksmų esamos būklės vaizdą: kurie pranešimai atviri ar uždari, kokie veiksmai laukia ir kiek kiekvieno tipo pranešimų buvo gauta. Šis procesas gali padėti nustatyti apsaugos problemas ir darbus išdėstyti pagal svarbą. Pagalbos pirmumo nustatymo metu surinkta informacija taip pat gali būti naudojama vyresniajai vadovybei skirtiems duomenims apie pažeidžiamumo ir incidentų tendencijas bei statistiniams duomenims rinkti [28].

Pagalbos pirmumo nustatymą turi atlikti tik labiausiai patyrę grupės nariai, kadangi tam reikia gerai suprasti galimą pažeidimo poveikį konkrečioms aptarnaujamų subjektų dalims ir gebėti nuspręsti, kuris grupės narys būtų tinkamas šiam incidentui tirti.

[27] Pagalbos pirmumo nustatymas „Vikipedijoje“: http://en.wikipedia.org/wiki/Triage.

[28] Incidentų valdymo procesų nustatymas: http://www.cert.org/archive/pdf/04tr015.pdf.

3 žingsnis: veiksmai

Paprastai pagal pirmumą suskirstyti incidentai įtraukiami į prašymų eilę incidentų valdymo programoje, kurią naudoja vienas ar keli incidentų tyrėjai, dažniausiai atliekantys toliau nurodytus veiksmus.

Incidento paraiškos numeris
Incidento paraiškos numeris jau galėjo būti priskirtas ankstesniame etape (pvz., kai apie incidentą buvo pranešta telefonu). Jei ne, pirmiausia reikia sukurti numerį, kuris bus naudojamas toliau bendraujant dėl šio incidento.

Incidento gyvavimo ciklas
Incidento tyrimas nėra tam tikri veiksmai, galiausiai lemiantys sprendimą. Tai daugiau ciklas veiksmų, kurie pakartotinai atliekami tol, kol pažeidimas galiausiai panaikinamas ir visos susijusios pusės gauna visą būtiną informaciją. Šį ciklą, dažnai dar vadinamą „incidento gyvavimo ciklu“, sudaro šie procesai:

Analizė: analizuojama visa informacija apie nurodytą incidentą.
Kontaktinės informacijos gavimas: kad būtų galima visoms susijusioms šalims, pavyzdžiui, kitoms CSIRT, nukentėjusiesiems ir galbūt savininkams sistemų, kurios galėjo būti piktybiškai panaudotos užpuolimui, toliau pranešti su pažeidimu susijusią informaciją.
Techninės pagalbos teikimas: padedama nukentėjusiesiems greitai panaikinti pažeidimo padarinius ir surinkti daugiau informacijos apie užpuolimą.
Koordinavimas: informuojamos kitos susijusios šalys, tokios kaip CSIRT, atsakingos už užpuolimui panaudotas IT sistemas, ar kiti nukentėjusieji.

Ši struktūra vadinama „gyvavimo ciklu“, kadangi vienas iš veiksmų lemia kitą, o paskutinis, koordinavimo dalies, vėl gali lemti naują analizę, ir ciklas vėl prasideda. Procesas baigiasi, kai visos susijusios šalys gauna ir praneša visą būtiną informaciją.

Išsamesnį incidento gyvavimo ciklo aprašymą rasite CERT/CC CSIRT atmintinėje[29].

Incidento tyrimo ataskaita
Parenkite ataskaitą – taip pasirengsite atsakyti į vadovybės klausimus apie incidentą. Taip pat labai naudinga parengti raštišką dokumentą (tik vidaus naudojimui) apie įgytą patirtį, skirtą darbuotojams mokyti ir padėsiantį išvengti klaidų incidentų valdymo procesuose ateityje.

Archyvavimas
Peržvelkite 6.6 dalyje „Informacijos apsaugos politikos kūrimas“ aprašytas archyvavimo taisykles.

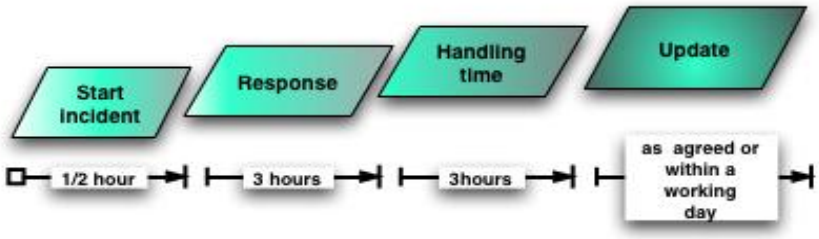
[29] CSIRT atmintinė: http

Išsamias rekomendacijas apie incidentų valdymą ir incidentų gyvavimo ciklą rasite priedo A.1 skirsnyje „Papildoma literatūra“.

Reagavimo tvarkaraščio pavyzdys

Reagavimo laikas dažnai nenustatomas, tačiau tai turi būti kiekvieno gerai sudaryto CSIRT ir jos aptarnaujamų subjektų paslaugos lygio susitarimo (SLA) dalis. Incidento tyrimo metu aptarnaujamiems subjektams savalaikiai pateikiamas atsakymas yra lemiamas ir aptarnaujamų subjektų įsipareigojimams, ir geram grupės vardui.
Atsakymo laikas aptarnaujamiems subjektams turi būti aiškiai nurodomas, kad būtų išvengta klaidingų lūkesčių. Toliau pateiktas labai paprastas tvarkaraštis gali būti naudojamas kaip atspirties taškas su CSIRT aptarnaujamais subjektais sudarant išsamesnį SLA.

Čia pateikiamas praktinio reagavimo nuo prašymo suteikti pagalbą gavimo momento tvarkaraščio pavyzdys:



16 pav. Reagavimo tvarkaraščio pavyzdys.

Dar labai naudinga aptarnaujamiems subjektams nurodyti jų pačių atsako laiką, ypač kai susisiekti su CSIRT reikia neatidėliotinai. Daugeliu atveju su savo CSIRT geriau susisiekti ankstyvame etape, todėl labai naudinga paskatinti aptarnaujamus subjektus daryti tai tuoj pat, kai tik kyla abejonių.

CSIRT naudojamos priemonės

Šiame skyriuje nurodomos kelios CSIRT grupių naudojamos priemonės. Jame pateikiami tik pavyzdžiai. Daugiau informacijos galima rasti tinklavietėje *Clearinghouse of Incident Handling Tools*[30] (CHIHT).

El. paštas ir laiškų šifravimo programinė įranga

- GNUPG http://www.gnupg.org/
  Programa GnuPG yra GNU projekto visapusiškas ir nemokamas OpenPGP standarto įgyvendinimas, kaip apibrėžta RFC 2440. Programa GnuPG galima šifruoti ir pasirašyti savo duomenis ir pranešimą.

- PGP http://www.pgp.com/
  Komercinis variantas

Incidentų valdymo programa

Valdo incidentus ir jų tolesnį tyrimą, palaikydama tikslią ir naujausią informaciją apie veiksmus.

- RTIR http://www.bestpractical.com/rtir/
  RTIR yra nemokama atviro šaltinio incidentų valdymo sistema, sukurta turint omenyje CERT tarnybas ir kitas incidentų reagavimo grupes.

CRM priemonės

Kai aptarnaujate daug įvairių subjektų ir reikia registruoti visus susitarimus ir informaciją, naudinga turėti CRM duomenų bazę. Yra daug įvairių variantų. Štai keletas pavyzdžių:

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

- „Sugarforce“ (nemokama atviro šaltinio versija) http://www.sugarforge.org/

Informacijos tikrinimas

- Tinklavietės stebėjimas
  http://www.aignes.com/index.htm
  Ši programa stebi tinklaviečių atnaujinimą ir pakeitimus.

- „Watch that page“ (Žiūrėkite šį puslapį)
  http://www.watchthatpage.com/
  Tarnyba el. paštu (nemokamu ir komerciniu) siunčia informaciją apie pasikeitimus tinklavietėse.

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

Kontaktinės informacijos radimas
Rasti teisingą adresatą, norint pranešti jam apie incidentus, nėra paprasta užduotis. Štai keli informacijos šaltiniai, kuriais galima pasinaudoti:

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

Be to, CHIHT sąraše yra kelios kontaktinės informacijos paieškos programos[34].

Išgalvota CSIRT (8 žingsnis)
Kuriamojo proceso eiga ir veiklos bei techninės procedūros Išgalvotos CSIRT tikslas – teikti pagrindines CSIRT paslaugas: • Perspėjimus ir įspėjimus • Pranešimus • Valdyti incidentus Grupė sukūrė procedūras, kurios veikia sklandžiai ir yra gerai suprantamos kiekvienam grupės nariui. Grupė taip pat pasamdė teisės specialistą, kuris užsiims įsipareigojimais ir informacijos apsaugos politika. Grupė išsirinko kelias naudingas programas ir, pasitarusi su kitomis CSIRT, rado naudingos informacijos apie veiklos aspektus. Buvo sukurtas nuolatinis apsaugos informacijos biuletenio ir pranešimų apie incidentus šablonas. Incidentams valdyti grupė naudoja RTIR sistemą.

[31] RIPE patikros priemonė „whois“: http://www.ripe.net/whois.

[32] Dokumentas „IRT-object“ RIPE duomenų bazėje“:
http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Patikimas teikėjas (angl. *Trusted Introducer*): http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] CHIHT naudojamos tapatybės tikrinimo priemonės: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 CSIRT mokymas

Jau žengėme šiuos žingsnius:

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.
2. Nustatėme, kokiam sektoriui nauja grupė teiks savo paslaugas.
3. Aptarėme paslaugas, kurias CSIRT gali teikti savo aptarnaujamiems subjektams.
4. Išanalizavome aplinką ir aptarnaujamus subjektus.
5. Apibrėžėme veiklą.
6. Sukūrėme verslo planą.
   a. Apibrėžėme finansinį modelį.
   b. Apibrėžėme organizacinę struktūrą.
   c. Pradėjome samdyti darbuotojus.
   d. Panaudojome biurą ir aprūpinome jį įranga.
   e. Sukūrėme informacijos apsaugos politiką.
   f. Ieškojome partnerių bendradarbiauti.
7. Parėmėme verslo planą.
   a. Buvo patvirtintas ekonominis modelis.
   b. Viską pritaikėme veiklos projekto planui.
8. Pradėjome CSIRT veiklą.
   a. Sukūrėme darbų srautus.
   b. Įdiegėme CSIRT priemones.

>> Kitas žingsnis: darbuotojų mokymas.

Šiame skyriuje nurodyti du pagrindiniai šaltiniai specializuotoms CSIRT mokyti: TRANSITS ir CERT/CC kursai.

TRANSITS

TRANSITS yra Europos projektas, skirtas tinklų ir informacijos saugumo incidentų reagavimo grupių (CSIRT) kūrimui skatinti ir veikiančioms CSIRT stiprinti, sprendžiant patyrusių CSIRT darbuotojų trūkumo problemą. Šio tikslo siekiama pateikiant specialistų rengimo kursus (naujų) CSIRT darbuotojams mokyti organizacinių, darbo, techninių, rinkos ir teisinių dalykų, susijusių su grupės teikiamomis paslaugomis.

Konkrečiai, TRANSITS

- tobulina, atnaujina ir reguliariai peržiūri modulinio rengimo kurso medžiagą;
- organizuoja mokymo seminarus, kai išsiunčiama kurso medžiaga;
- suteikia galimybę (naujų) CSIRT grupių personalo nariams dalyvauti šiuose mokomuosiuose seminaruose, ypač pabrėždama narių iš ES šalių kandidačių dalyvavimą;
- skleidžia mokymo kursų medžiagą ir užtikrina rezultatų panaudojimą[35].

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

ENISA palengvina ir remia TRANSITS kursus. Jei norite sužinoti, kaip kreiptis dėl kursų, reikalavimus ir kainą, susisiekite su ENISA CSIRT ekspertais adresu

CERT-Relations@enisa.europa.eu

Šio dokumento priede yra mokomojo kurso medžiagos pavyzdys!

CERT/CC

Dėl kompiuterių ir tinklų infrastruktūros sudėtingumo bei sunkaus jų valdymo nelengva tinkamai užtikrinti tinklų saugumą. Tinklų ir sistemų administratoriai neturi pakankamai žmonių ir taikomos saugumo praktikos, kad galėtų apsisaugoti nuo pažeidimų ir sumažinti žalą. Todėl kompiuterinių saugumo incidentų skaičius didėja.
Įvykus kompiuteriniam saugumo incidentui, organizacijos turi reaguoti greitai ir veiksmingai. Kuo greičiau organizacija atpažįsta, išanalizuoja ir reaguoja į incidentą, tuo geriau gali apriboti žalą ir sumažinti padarinių panaikinimo išlaidas. Tinklų ir informacijos saugumo incidentų reagavimo grupės (CSIRT) įkūrimas yra puikus būdas įgyti greito reagavimo pajėgumus, taip pat kaip ir pagalbą užkertant kelią incidentams ateityje.

CERT-CC vadovams ir techniniam personalui siūlo kursus tokių sričių kaip tinklų ir informacijos saugumo incidentų reagavimo grupių (CSIRT) kūrimas, reagavimas į saugumo incidentus ir jų tyrimas bei tinklų saugumo gerinimas. Jei nepranešama kitaip, visi kursai organizuojami Pitsburge (*Pittsburgh*), Pensilvanijos valstijoje. Mūsų personalo nariai taip pat dėsto saugumo kursą Karnegio Melono universitete (*Carnegie Mellon University*)

CSIRT grupėms skirti CERT/CC kursai[36]

Tinklų ir informacijos saugumo incidentų reagavimo grupės (CSIRT) kūrimas
Tinklų ir informacijos saugumo incidentų reagavimo grupių (CSIRT) valdymas
Incidentų valdymo pagrindai
Sudėtingesnis incidentų valdymas techniniam personalui

Šio dokumento priede yra mokomojo kurso medžiagos pavyzdys!

Išgalvota CSIRT (9 žingsnis)
Darbuotojų mokymas Išgalvota CSIRT nusprendžia visus savo techninius darbuotojus nusiųsti į būsimus TRANSITS kursus. Grupės vadovas papildomai lanko CERT/CC parengtą „Vadovavimo CSIRT“ kursą.

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

10 Pratybos: informacinio biuletenio kūrimas

Jau žengėme šiuos žingsnius:

1. Išsiaiškinome, kas yra CSIRT ir kokia jos nauda.
2. Nustatėme, kokiam sektoriui nauja grupė teiks savo paslaugas.
3. Aptarėme paslaugas, kurias CSIRT gali teikti savo aptarnaujamiems subjektams.
4. Išanalizavome aplinką ir aptarnaujamus subjektus.
5. Apibrėžėme veiklą.
6. Sukūrėme verslo planą.
   a. Apibrėžėme finansinį modelį.
   b. Apibrėžėme organizacinę struktūrą.
   c. Pradėjome samdyti darbuotojus.
   d. Panaudojome biurą ir aprūpinome jį įranga.
   e. Sukūrėme informacijos apsaugos politiką.
   f. Ieškojome partnerių bendradarbiauti.
7. Parėmėme verslo planą.
   a. Buvo patvirtintas ekonominis modelis.
   b. Viską pritaikėme veiklos projekto planui.
8. Pradėjome CSIRT veiklą.
   a. Sukūrėme darbų srautus.
   b. Įdiegėme CSIRT priemones.
9. Mokėme darbuotojus.

>> Kitas žingsnis – praktikuotis ir pasirengti tikram darbui!

Šiame skyriuje pateikiamas kasdienės CSIRT užduoties – informacinio biuletenio – kūrimo pratimo pavyzdys.

Tai padaryti paskatino šis „Microsoft“ išsiųstas originalus apsaugos biuletenis:

Biuletenio identifikatorius	**„Microsoft“ apsaugos biuletenis MS06-042**
Biuletenio pavadinimas	**Sudėtinis „Internet Explorer“ apsaugos atnaujinimas (918899)**
Santrauka	Šis atnaujinimas panaikina kelias silpnas „Internet Explorer“ vietas, kuriomis pasinaudojus būtų galima kodą paleisti nuotoliniu būdu.
Didžiausio sunkumo vertinimas	Kritinis
Pažeidžiamumo poveikis	Nuotolinis kodo paleidimas
Paveikta programinė įranga	**„Windows, Internet Explorer“.** Daugiau informacijos rasite skirsnyje „Paveikta programinė įranga ir parsisiuntimo vietos“.

Šis gamintojo pranešimas atkreipia dėmesį į neseniai aptiktą „Internet Explorer“ pažeidžiamumą. Gamintojas paskelbia kelis šios programos pataisymus, skirtus įvairioms „Microsoft Windows“ sistemos versijoms.

Išgalvota CSIRT, pagal adresatų sąrašą gavusi informaciją apie šį pažeidžiamumą, pradeda darbų srautą, aprašytą 8.2 skyriuje „Perspėjimų, įspėjimų ir pranešimų kūrimas“.

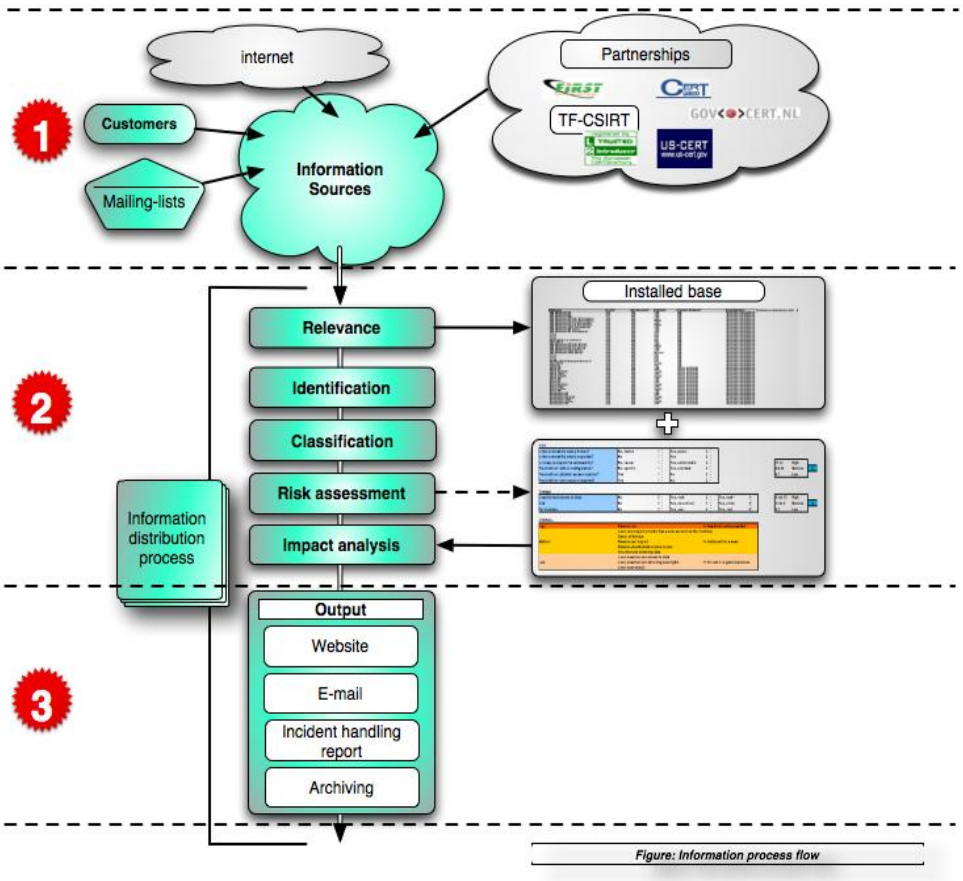


Figure: Information process flow

1 žingsnis: informacijos apie sistemų pažeidžiamumą rinkimas.

Pirmiausia peržiūrima gamintojo tinklavietė. Taip išgalvota CSIRT patvirtina informacijos autentiškumą ir surenka papildomus duomenis apie pažeidžiamumą ir paveiktas IT sistemas.

2 žingsnis: informacijos analizė ir rizikos vertinimas

Identifikavimas
Informacija jau buvo patvirtinta atlikus kryžminę informacijos apie pažeidžiamumą, gautos el. paštu, kuriame buvo tekstas apie gamintojo tinklavietę, kontrolę.

Tinkamumas
Išgalvota CSIRT tinklavietėje rastų paveiktų sistemų sąrašą palygina su aptarnaujamo subjekto naudojamų sistemų sąrašu. Ji nustato, kad mažiausiai vienas aptarnaujamas subjektas naudoja „Internet Explorer“, taigi informacija apie pažeidžiamumą tikrai tinkama.

Kategorija	Pritaikymas	Programinė įranga	Versija	OS	OS Versija	Aptarnauja-mas subjektas
Stalinis kompiuteris	Naršyklė	IE	x-x-	„Microsoft“	„XP-prof“	A

Klasifikavimas
Informacija yra vieša, todėl ją galima naudoti ir perskirstyti.

Rizikos vertinimas ir poveikio analizė
Atsakymai į klausimus rodo, kad rizika ir poveikis yra *dideli* („Microsoft“ vertino juos kaip *kritinius*)

RIZIKA

Ar pažeidžiamumas gerai žinomas?	Taip
Ar šis pažeidžiamumas plačiai paplitęs?	Taip
Ar lengva pasinaudoti pažeidžiamumu?	Taip
Ar šiuo pažeidžiamumu galima pasinaudoti nuotoliniu būdu?	Taip

ŽALA
Galimas poveikis yra nuotolinė prieiga ir galimas kodo paleidimas nuotoliniu būdu. Šis pažeidžiamumas apima kelis aspektus, dėl to žalos rizika *didelė*.

3 žingsnis: Paskirstymas

Išgalvota CSIRT yra vidaus CSIRT. Ji turi el. paštą, telefoną ir vidinę tinklavietę, naudojamus kaip ryšio kanalus. Pasinaudodama 8.2 skyriuje „Perspėjimų, įspėjimų ir pranešimų kūrimas“ pateiktu šablonu, CSIRT parengia šį informacinį biuletenį.

Biuletenio pavadinimas
Silpnos programos „Internet Explorer“ vietos

Nuorodos numeris
082006-1

Pažeistos sistemos

- Visos stalinio kompiuterio sistemos, kurios paleidžia „Microsoft“ programas

Susijusi OS ir versija

- „Microsoft Windows 2000 Service Pack 4“
- „Microsoft Windows XP Service Pack 1„ ir „Microsoft Windows XP Service Pack 2“
- „Microsoft Windows XP Professional x64 Edition“
- „Microsoft Windows Server 2003“ ir „Microsoft Windows Server 2003 Service Pack 1“
- „Microsoft Windows Server 2003“, skirta „Itanium“ technologijų sistemoms ir „Microsoft Windows Server 2003“ su SP1, skirta „Itanium“ technologijų sistemoms
- „Microsoft Windows Server 2003 x64 Edition“

Rizika (didelė, vidutinė, maža)
DIDELĖ

Poveikis/galima žala (didelė, vidutinė, maža)
DIDELĖ

Išoriniai ID: (CVE, pažeidžiamumo biuletenių ID)
MS-06-42

Pažeidžiamumo apžvalga
„Microsoft“ aptiko kelias kritines silpnas programos „Internet Explorer“ vietas, kuriomis galima pasinaudoti kodui paleisti nuotoliniu būdu.

Poveikis
Puolantysis gali visiškai valdyti sistemą, įdiegdamas programas, prijungdamas papildomus naudotojus, ir varžytis, pakeisti ar panaikinti duomenis. Lengvinantis veiksnys yra tai, kad pirmiau nurodytas pažeidimas gali būti vykdomas tik tuo atveju, jei naudotojas registruojamas į seansą administratoriaus teisėmis. Naudotojams, prisijungusiems mažesnėmis teisėmis, poveikis galėtų būti mažesnis.

Sprendimas
Nedelsiant taisykite savo IE (Internet Explorer) programą.

Aprašymas (išsamus)
Daugiau informacijos rasite ms06-042.mspx

Priedėlis
Daugiau informacijos rasite ms06-042.mspx

Šį dokumentą jau galima išplatinti. Kadangi tai labai svarbus biuletenis, kai įmanoma, patartina taip pat paskambinti aptarnaujamiems subjektams.

Išgalvota CSIRT (10 žingsnis)
Pratybos Pirmomis veiklos savaitėmis išgalvota CSIRT pratyboms naudojo kelis netikrus atvejus (jų pavyzdžius gavo iš kitų CSIRT). Be to, grupė išleido kelis tikra aparatinės ir programinės įrangos gamintojų išplatinta informacija apie pažeidžiamumą pagrįstus saugumo biuletenius, kuriuos tiksliai pritaikė aptarnaujamų subjektų poreikiams.

11 Išvada

Čia rekomendacijos baigiamos. Šis dokumentas skirtas glaustai apžvelgti įvairius procesus, būtinus kuriant CSIRT. Juo nesiekiama paaiškinti visko arba per daug įsigilinti į konkrečias smulkmenas. Priedo A.1 skirsnyje „Papildoma literatūra“ šia tema rasite medžiagos, kurią verta perskaityti.

Dabar išgalvota CSIRT turėtų žengti kitą svarbų žingsnį:

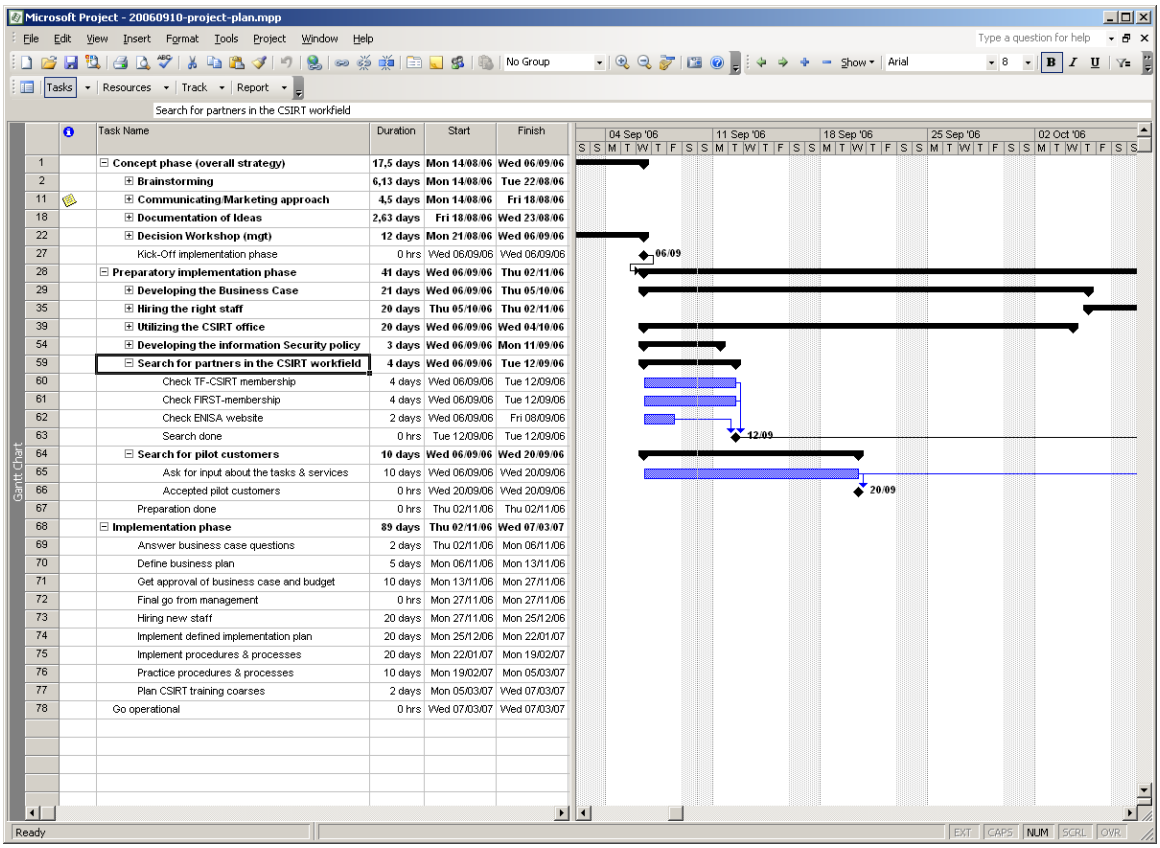
- Gauti aptarnaujamų subjektų atsiliepimus, kad galėtų tiksliai pritaikyti teikiamas paslaugas
- Nustatyti kasdienio darbo tvarką
- Atlikti avarinių situacijų pratybas
- Palaikyti glaudžius ryšius su įvairiomis CSIRT bendruomenėmis, turint tikslą vieną dieną prisidėti prie jų savanoriško darbo

12 Veiklos projekto plano aprašymas

PASTABA: veiklos projekto planas yra pirmas jam vykdyti būtino laikotarpio vertinimas. Priklausomai nuo turimų išteklių, tikra projekto trukmė gali būti įvairi.

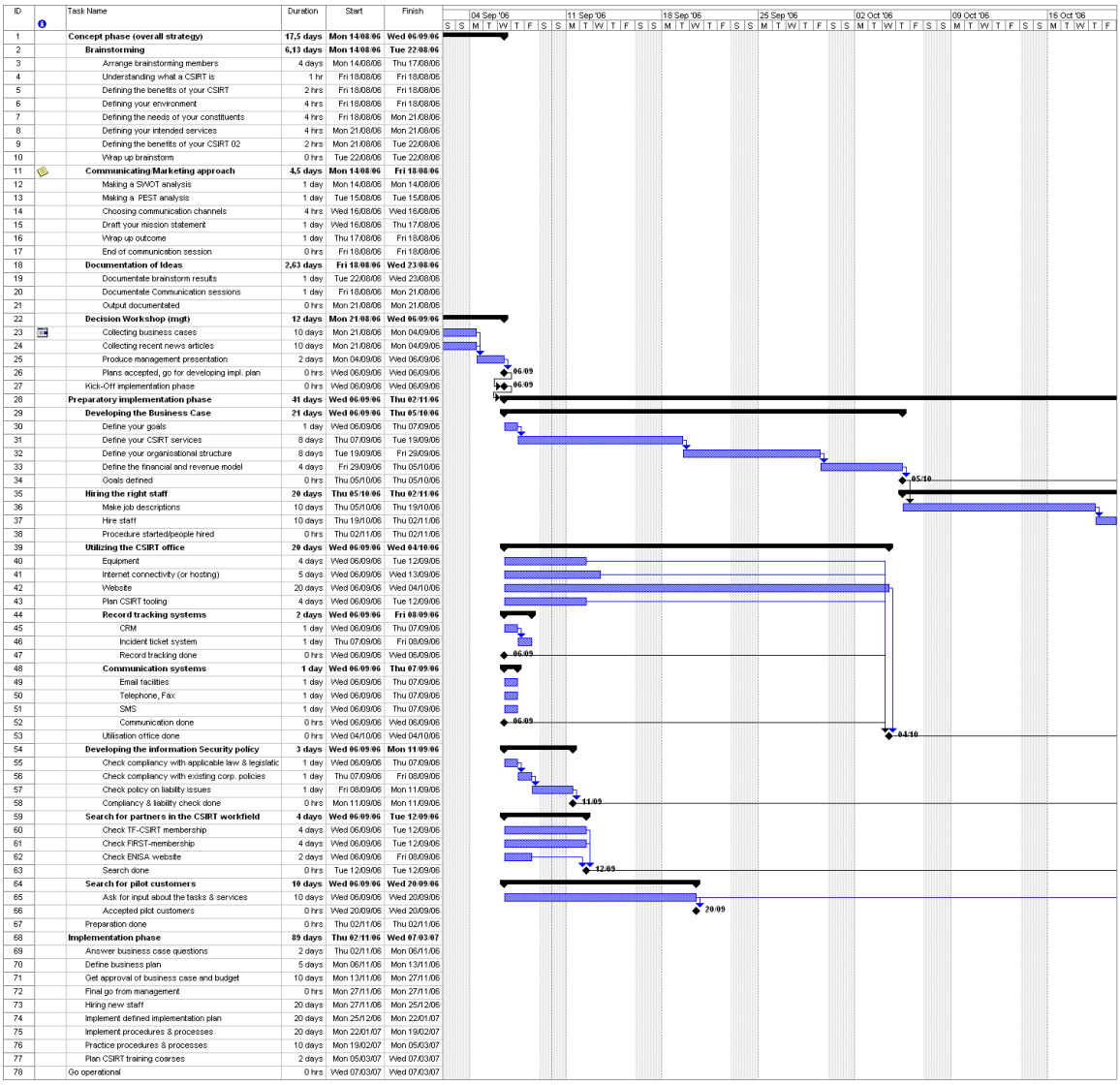
Veiklos projekto planas įvairiais formatais pateikiamas kompaktiniame diske ir ENISA tinklavietėje. Jis visiškai apima visus šiame dokumente aprašytus procesus.

Pagrindinis formatas yra „Microsoft Project“, kad jį būtų galima tiesiogiai naudoti šia projekto valdymo programa.



	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

17 pav. Veiklos projekto planas.



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

18 pav. Veiklos projekto planas su visomis užduotimis ir kalendorinio grafiko (Gantt chart) dalimi.

Veiklos projekto planas taip pat yra CVS ir XML formatų. Kitų formatų galima paprašyti ENISA CSIRT ekspertų: CERT-Relations@enisa.europa.eu

PRIEDAS

A.1 Papildoma literatūra

Handbook for CSIRTs (CERT/CC) (CSIRT atmintinė (CERT/CC).)
Labai plati su CSIRT darbu susijusių temų nuorodų rinktinė
Šaltinis: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress (Incidentų valdymo procesų CSIRT grupėms nustatymas: nebaigtas darbas.)
Išsami incidentų valdymo analizė.
Šaltinis: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs) (Tinklų ir informacijos saugumo incidentų reagavimo grupių (CSIRT) praktikos padėtis.)
Išsami tikros CSIRT išsidėstymo visame pasaulyje padėties, įskaitant istoriją, statistinius duomenis ir daug kitų dalykų, analizė.
Šaltinis: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box (CERT dėžutėje.)
Visapusiškas patirties, įgytos steigiant GOVCERT.NL ir Danijos nacionalinę informacijos tarnybą „De Waarschuwingsdienst“, apibūdinimas.
Šaltinis: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response (Lūkesčiai dėl reagavimo į kompiuterinio saugumo incidentus.)
Šaltinis: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide (NIST kompiuterinių saugumo incidentų valdymo vadovas.)
Šaltinis: http://www.securityunit.com/publications/sp800-61.pdf

ENISA Inventory of CERT activities in Europe (ENISA „CERT veiklos Europoje apžvalga.)
Nuorodų sąrašas, kuriame yra informacijos apie Europos CSIRT grupes ir įvairią jų veiklą.
Šaltinis: http://www.enisa.europa.eu/cert_inventory/

[37] Nacionalinis standartų ir technologijų institutas (angl. *National Institute of Standards and Technologies*).

A.2 CSIRT paslaugos

Nuoširdžiai dėkojame CERT/CC, pateikusiai šį sąrašą.

Reaktyviosios paslaugos	***Iniciatyviosios paslaugos***	***Artefaktų valdymas***
• Perspėjimai ir įspėjimai • Incidentų valdymas • Incidentų analizė • Reagavimas į incidentus vietoje • Reagavimo į incidentus pagalba • Reagavimo į incidentus koordinavimas • Pažeidžiamumo valdymas • Pažeidžiamumo analizė • Reagavimas į pažeidžiamumą • Reagavimo į pažeidžiamumą koordinavimas	• Pranešimai • Technologijos naujovių sekimas • Apsaugos auditas arba vertinimas • Apsaugos konfigūravimas ir priežiūra • Apsaugos priemonių tobulinimas • Įsibrovimo aptikimo paslaugos • Su sauga susijusios informacijos skleidimas	• Artefaktų analizė • Reagavimas į artefaktus • Reagavimo į artefaktus koordinavimas ***Apsaugos kokybės valdymas*** • Rizikos analizė • Verslo tęstinumas ir sutrikimo padarinių šalinimas • Konsultavimas saugos klausimais • Informacijos skleidimas • Švietimas/mokymas • Produkto vertinimas arba sertifikavimas

19 pav. CERT/CC sudarytas CSIRT paslaugų sąrašas.

Paslaugų

Reaktyviosios paslaugos

Šios paslaugos skirtos reaguoti į CSIRT aptarnaujamų subjektų pagalbos prašymus, pranešimus apie incidentus ir visas CSIRT sistemoms kylančias grėsmes bei užpuolimus. Kai kurias paslaugas gali inicijuoti trečiųjų šalių pranešimai arba stebėsenos ar IDS žurnalų ir perspėjimų apžvalga.

Perspėjimai ir įspėjimai

Ši paslauga apima informacijos, apibūdinančios įsilaužėlio puolimą, saugos pažeidžiamumą, perspėjimą apie įsilaužimą, kompiuterinį, arba netikrą (HOAX), virusą, skleidimą ir rekomendacijas, kokių veiksmų imtis, norint greitai pašalinti kylančią problemą. Perspėjimas, įspėjimas ar informacinis biuletenis siunčiami reaguojant į esamą problemą, norint aptarnaujamiems subjektams pranešti apie veiksmus ir pateikti rekomendacijas, kaip apsaugoti savo sistemas ar pataisyti tas, kurios buvo pažeistos. Informaciją gali sukurti CSIRT arba perskirstyti gamintojai, kitos CSIRT ar saugos specialistai, arba kitos aptarnaujamų subjektų dalys.

Incidentų valdymas

Incidentų valdymas apima prašymų ir pranešimų gavimą, pirmumo nustatymą ir reagavimą bei incidentų ir įvykių analizę. Tam tikra reagavimo veikla gali būti:

- apsaugoti sistemas ir tinklus, kuriuos paveikė įsilaužėlio veikla arba kuriems kilo tokia grėsmė;
- susijusiuose informaciniuose biuleteniuose arba perspėjimuose pateikti sprendimus ir pažeidimo sušvelninimo strategijas;
- ieškoti įsilaužėlio veiklos kitose tinklo dalyse;
- filtruoti tinklo srautą;
- atkurti sistemas;
- taisyti sistemas;
- kurti kitas reagavimo ar triktį kompensuojančių veiksmų strategijas.

Kadangi incidentus įvairiais metodais valdo įvairių tipų CSIRT, toliau ši paslauga, remiantis atliktos veiklos ir suteiktos pagalbos tipu, kategorijomis skirstoma taip:

Incidento analizė

Yra daug incidentų analizės lygių ir papildomų paslaugų. Iš esmės, incidento analizė yra visos turimos informacijos ir patvirtinamųjų dokumentų ar artefaktų, susijusių su incidentu ar įvykiu, tyrimas. Analizės tikslas – nustatyti incidento veikimo sritį, sukeltos žalos mastą, jo pobūdį ir esamas reagavimo strategijas arba triktį kompensuojančius veiksmus. CSIRT gali naudoti pažeidžiamumo ir artefaktų analizės (apibūdinta toliau) rezultatus, kad suprastų, kas įvyko konkrečioje sistemoje, ir atliktų visapusišką ir naujausią tų įvykių tyrimą. CSIRT susieja su incidentais susijusius veiksmus, kad nustatytų visus sąryšius, tendencijas, struktūras ar įsilaužėlio parašus. Dvi papildomos paslaugos, kurios, priklausomai nuo CSIRT paskirties, tikslų ir procesų, gali būti teikiamos kaip incidento analizės dalis, yra:

Kaltės įrodymų rinkimas

Įrodymų iš įsilaužtos kompiuterio sistemos rinkimas, saugojimas, dokumentavimas ir tyrimas, siekiant nustatyti sistemos pokyčius ir padėti atkurti įvykius, lemiančius saugumo pažeidimą. Informaciją ir duomenis reikia rinkti taip, kad dokumentais būtų patvirtinta įrodoma saugojimo grandinė, teismo leistina pagal įrodinėjimo taisykles. Renkant kaltės įrodymus, atliekamos užduotys apima (bet neapsiriboja) paveiktos sistemos kietojo disko dvejetainiu kodu išreikšto vaizdo kopijavimą; sistemos pakeitimų, tokių kaip naujos programos, failai, paslaugos ir vartotojai, buvimo tyrimą; vykdomų procesų ir atvirų prievadų tikrinimą; „Trojos arklio“ programų ir programuotojo paketų buvimo tyrimą. Šią funkciją atliekantiems CSIRT darbuotojams taip pat gali reikėti būti pasirengusiems teismo procesų metu būti ekspertais liudytojais.

Sekimas arba suradimas

Įsilaužėlio kilmės suradimas arba sistemų, prie kurių įsilaužėlis turi prieigą, nustatymas. Ši veikla gali apimti sekimą arba suradimą, kaip įsilaužėlis pateko į paveiktas sistemas ir susijusius tinklus, kurios sistemos buvo panaudotos šiai prieigai gauti, kur užpuolimas prasidėjo ir kokios kitos sistemos ir tinklai buvo panaudoti kaip užpuolimo dalis. Šio proceso metu taip pat gali būti bandoma nustatyti įsilaužėlio tapatybę. Šį darbą galima atlikti savarankiškai, tačiau dažniausiai dirbama kartu su teisėsaugos darbuotojais, interneto paslaugų teikėjais ir kitomis susijusiomis organizacijomis.

Reagavimas į incidentus vietoje

CSIRT teikia tiesioginę pagalbą vietoje, kad padėtų aptarnaujamiems subjektams atitaisyti incidento padarinius. CSIRT darbuotojai patys fiziškai tiria paveiktas sistemas ir taiso jas bei atnaujina, užuot incidentų reagavimo pagalbą teikę tik telefonu ar el. paštu (žr. apačioje). Ši paslauga apima visus vietos lygiu atliekamus veiksmus, kurie yra būtini, jei incidento tikimasi arba jis įvyko. Jei CSIRT nėra įsikūrusi ten, kur įvyko pažeidimas, grupės nariai vyksta į tą vietą ir atlieka reagavimo veiksmus. Kitais atvejais vietos grupė jau gali būti ten įsikūrusi ir reagavimo į incidentą veiksmus atlieka kaip savo įprastinį darbą. Tai ypač taikytina, kai už įkurtą CSIRT incidento valdymo funkciją, kaip savo įprastinio darbo dalį, atlieka sistemos, tinklo ar saugos administratoriai.

Reagavimo į incidentus pagalba

Užpuolimo aukoms CSIRT telefonu, el. paštu, faksu ar dokumentais pataria ir padeda atitaisyti incidento padarinius. Tai gali būti techninė pagalba išaiškinant surinktus duomenis, kontaktinės informacijos teikimas ar rekomendacijų dėl sušvelninimo ir atkūrimo strategijų perdavimas. Anksčiau minėti tiesioginiai incidentų reagavimo veiksmai vietoje neatliekami. Šiuo atveju CSIRT rekomendacijas teikia nuotoliniu būdu, kad vietos darbuotojai sistemas atkurti galėtų patys.

Reagavimo į incidentus koordinavimas

CSIRT koordinuoja incidente dalyvaujančių šalių reagavimo pastangas. Tai paprastai būna užpuolimo auka, kiti su incidentu susiję objektai ir bet kokie objektai, kuriems reikia padėti ištirti užpuolimą. Tai taip pat gali apimti objektus, teikiančius IT pagalbą aukoms, tokius kaip interneto paslaugų teikėjai, kitos CSIRT ir objekto sistemos bei tinklo administratoriai. Koordinavimo darbas gali apimti kontaktinės informacijos rinkimą, objektų įspėjimą apie galimą jų įtraukimą (kaip aukų ar užpuolimo šaltinių), statistinių duomenų apie įtrauktų objektų skaičių rinkimą ir keitimosi informacija bei jos analizės palengvinimą. Koordinavimo darbo dalimi gali būti pranešimų teikimas ir bendradarbiavimas su organizacijos teisininkais, žmogiškųjų išteklių ar viešųjų ryšių skyriais. Tai taip pat apima ir veiksmų derinimą su teisėtvarkos darbuotojais. Ši paslauga neapima tiesioginio reagavimo į incidentą vietoje.

Pažeidžiamumo valdymas

Pažeidžiamumo valdymas – tai informacijos ir pranešimų apie aparatinės ir programinės įrangos silpnas vietas gavimas; silpnų vietų pobūdžio, mechanizmo ir poveikio analizė; silpnų vietų aptikimui ir taisymui skirtų reagavimo strategijų tobulinimas. Kadangi pažeidžiamumą įvairiais metodais valdo įvairių tipų CSIRT, toliau ši paslauga, remiantis atliktos veiklos ir suteiktos pagalbos tipu, kategorijomis skirstoma taip:

Pažeidžiamumo analizė

CSIRT atlieka techninę aparatinės ar programinės įrangos silpnų vietų analizę ir tyrimą. Tai apima įtartinų silpnų vietų patikrą ir techninį aparatinės ar programinės įrangos pažeidžiamumo tyrimą, siekiant nustatyti, kur jo esama ir kaip jis gali būti išnaudotas. Analizė gali apimti šaltinio kodo peržiūrą, naudojant derinimo programą, siekiant aptikti, kur atsirado pažeidžiamumas, arba bandant atkurti problemą tyrimo sistemoje.

Reagavimas į pažeidžiamumą

Ši paslauga apima atitinkamo reagavimo nustatymą, siekiant sumažinti ar pataisyti pažeidžiamumą. Tai gali būti pataisų, taisymo ir triktį kompensuojančių veiksmų tobulinimas ar tyrimas. Dar gali būti kitiems pranešama apie trūkumų mažinimo strategiją, galbūt sukuriant ir platinant biuletenius ar perspėjimus. Be to, reagavimo veiksmai gali būti pataisų, taisymų įdiegimas ar triktį kompensuojantys veiksmai.

Reagavimo į pažeidžiamumą koordinavimas

Įvairioms įmonės ar aptarnaujamų subjektų dalims CSIRT praneša apie pažeidžiamumą ir dalijasi informacija apie tai, kaip taisyti ar sumažinti pažeidžiamumą. CSIRT patvirtina, kad reagavimo į pažeidžiamumą strategija yra sėkmingai įgyvendinama. Ši paslauga gali apimti ryšius su pardavėjais, kitomis CSIRT, techniniais ekspertais, aptarnaujamų subjektų nariais ir asmenimis ar grupėmis, kurios nuo pat pradžių aptiko pažeidžiamumą ar pranešė apie jį. Tai gali būti pažeidžiamumo ar pranešimo apie jį analizės palengvinimas; atitinkamų dokumentų išleidimo, pataisų ar triktį kompensuojančių veiksmų atlikimo tvarkaraščio koordinavimas; įvairių šalių atlikto techninio tyrimo apibendrinimas. Ši paslauga taip pat gali apimti pažeidžiamumo informacijos ir atitinkamų reagavimo strategijų viešojo arba privataus archyvo ar žinių bazės priežiūrą.

Artefaktų valdymas

Artefaktai yra visi sistemoje randami failai ar objektai, kurie galėtų būti panaudoti sistemoms ir tinklams žvalgyti ar užpulti, arba kurie naudojami sužlugdyti saugos priemones. Artefaktai gali būti, tačiau tuo neapsiriboja, kompiuterių virusai, „Trojos arklio“ programos, „kirminai“, įsilaužimo scenarijai ir programuotojo paketai.
Artefaktų valdymas apima informacijos apie artefaktus, kurie naudojami įsilaužėlių užpuolimams, žvalgybai ir kitai neleistinai ar ardomajai veiklai, ir jų kopijų gavimą. Gautas artefaktas peržiūrimas. Tai apima artefaktų pobūdžio, mechanikos, versijos ir naudojimo analizę; reagavimo strategijų, skirtų šiems artefaktams aptikti, pašalinti ir nuo jų apsisaugoti kūrimą (arba pasiūlymą). Kadangi artefaktus įvairiais metodais valdo įvairių tipų CSIRT, toliau ši paslauga, remiantis atliktos veiklos ir suteiktos pagalbos tipu, kategorijomis skirstoma taip:

Artefakto analizė

CSIRT atlieka visų sistemoje randamų artefaktų techninį tyrimą ir analizę. Analizė gali apimti artefakto failo tipo ir struktūros nustatymą, palyginant naują artefaktą su esančiais arba kitomis to paties artefakto versijomis, kad būtų galima pamatyti panašumus ir skirtumus, arba apgrąžos technologiją ar išrinkimo kodą, siekiant nustatyti artefakto tikslą ir funkciją.

Reagavimas į artefaktą

Teikiant šią paslaugą, apibrėžiami atitinkami artefakto aptikimo ir pašalinimo iš sistemos veiksmai, taip pat imamasi artefaktų įdiegimui kelią užkertančių priemonių. Tai gali būti kūrimas parašų, kuriais papildomos antivirusinės ar IDS programos.

Reagavimo į artefaktą koordinavimas

Ši paslauga apima su artefaktu susijusios analizės rezultatų apibendrinimą ir dalijimąsi jais bei reagavimo strategijomis su kitais tyrėjais, CSIRT grupėmis, gamintojais ir kitais saugos specialistais. Atliekant šiuos darbus, siunčiami pranešimai kitiems ir

apibendrinami techninių tyrimų rezultatai, gauti iš įvairių šaltinių. Tai taip pat gali būti viešųjų ar aptarnaujamų subjektų žinomų artefaktų ir jų poveikio bei atitinkamų reagavimo strategijų archyvų priežiūra.

Iniciatyviosios paslaugos

Iniciatyviosios paslaugos yra skirtos aptarnaujamų subjektų infrastruktūrai ir saugos procesams gerinti anksčiau nei įvyksta arba aptinkamas incidentas ar įvykis. Pagrindinis tikslas – išvengti incidentų, o jiems kilus – sumažinti jų poveikį ir apimtį.

Pranešimai

Jie apima perspėjimus apie įsilaužimus, įspėjimus apie pažeidžiamumą ir saugos biuletenius, tačiau jais neapsiriboja. Tokiais pranešimais aptarnaujami subjektai informuojami apie naujus įvykius, turinčius vidutinės trukmės ar ilgalaikio poveikio, pavyzdžiui, naujai rastos silpnos vietos ar įsilaužėlio programos. Aptarnaujamiems subjektams pranešimai suteikia galimybę apsaugoti savo sistemas ir tinklus nuo naujai rastų problemų anksčiau nei jos galėtų būti panaudotos.

Technologijos naujovių sekimas

CSIRT stebi ir peržvelgia technologijos naujoves, įsilaužėlių veiklą ir susijusias tendencijas, kad padėtų nustatyti būsimą grėsmę. Peržiūrėtos temos gali būti praplečiamos ir papildomos teisiniais ir teisės aktų leidimo sprendimais, socialinėmis ar politinėmis grėsmėmis ir naujausiomis technologijomis Ši paslauga apima saugos adresatų sąrašų, apsaugos tinklaviečių ir naujausių žinių bei žurnalų straipsnių mokslo, technologijų, politikos ir vyriausybės veiklos srityse skaitymą, siekiant išrinkti su aptarnaujamų subjektų sistemų ir tinklų sauga susijusią informaciją. Tai gali būti bendravimas su kitomis šalimis, kurios yra šių sričių valdymo institucijos, siekiant užtikrinti, kad būtų gaunama geriausia ir tiksliausia informacija ar išaiškinimas. Šios paslaugos rezultatas galėtų būti kurio nors tipo pranešimas, rekomendacijos ar patarimai, daugiau akcentuojantys vidutinės trukmės ar ilgalaikius saugos aspektus.

Saugos auditas arba vertinimas

Teikiant šią paslaugą, organizacijos saugos infrastruktūra visapusiškai patikrinama ir analizuojama remiantis organizacijos ar kitų verslo šakos taikomų standartų nustatytais reikalavimais. Dar gali būti atliekama organizacijos saugos užtikrinimo praktikos apžvalga. Gali būti atliekami įvairūs auditai arba patikros, įskaitant toliau nurodytąsias.

Infrastruktūros peržiūra

Rankiniu būdu patikrinamos aparatinės ir programinės įrangos konfigūracijos, maršrutizatoriai, ugniasienės, serveriai ir stalinių kompiuterių įtaisai, siekiant užtikrinti, kad jie atitiktų geriausią organizacijos ar verslo šakos saugos politikos ir standartinių konfigūracijų praktiką.

Geriausios praktikos peržiūra

Atliekama darbuotojų ir sistemos bei tinklų administratorių apklausa, siekiant nustatyti, ar jų apsaugos praktika atitinka nustatytą organizacijos saugos politiką arba konkrečius verslo šakos standartus.

Paieška

Naudojamos pažeidžiamumo ar virusų paieškos programos, siekiant nustatyti, kurios sistemos ir tinklai yra pažeidžiami.

Prasiskverbimo bandymas

Objekto sauga išbandoma sąmoningai užpuolant jo sistemas ir tinklus.
Prieš atliekant minėtus auditus ar vertinimus, reikia gauti vyresniosios vadovybės leidimą. Organizacijos politika gali drausti taikyti kai kuriuos iš šių metodų. Teikiant šią paslaugą, gali būti kuriama bendra bandymų ar vertinimo praktikos taikymo sistema, taip pat formuojama reikiamų įgūdžių visuma arba sertifikavimo reikalavimai, skirti bandymus, vertinimą, auditus ar peržiūras atliekantiems darbuotojams. Šią paslaugą taip pat galima perduoti sutartį pasirašiusiai trečiajai šaliai arba valdomam apsaugos paslaugos teikėjui, turinčiam atitinkamą kvalifikaciją auditų ir vertinimo srityje.

Apsaugos priemonių, taikomųjų programų, infrastruktūrų ir paslaugų konfigūravimas ir priežiūra

Teikiant šią paslaugą, nustatomi arba teikiami atitinkami nurodymai, kaip saugiai konfigūruoti ir prižiūrėti priemones, taikomąsias programas ir bendrą skaitmeninę infrastruktūrą, kurią naudoja CSIRT aptarnaujami subjektai ar pati CSIRT. Be rekomendacijų teikimo, CSIRT gali atlikti konfigūravimo atnaujinimus ir apsaugos priemonių bei paslaugų, tokių kaip IDS, tinklų peržiūros ar sistemų stebėsena, filtrai, apvalkalai, ugniasienės, virtualieji privatūs tinklai (VPN) ar autentikavimo mechanizmai, priežiūrą. Šios paslaugos netgi gali sudaryti CSIRT pagrindinės funkcijos dalį. Laikydamasi saugos nurodymų, CSIRT taip pat gali konfigūruoti ir prižiūrėti serverius, stalinius, nešiojamuosius ir delninius (PDA) kompiuterius bei kitus belaidžius prietaisus. Ši paslauga apima pranešimus vadovybei apie visas su priemonių ir programų konfigūravimu ar naudojimu susijusias problemas ir aspektus, dėl kurių, CSIRT nuomone, sistema galėtų būti neapsaugota nuo užpuolimo.

Apsaugos priemonių kūrimas

Ši paslauga apima naujų, specifinių aptarnaujamiems subjektams priemonių, kurių reikia arba nori aptarnaujami subjektai arba pati CSIRT, kūrimą. Pavyzdžiui, tai gali būti apsaugos pataisų pritaikytai aptarnaujamų subjektų programinei įrangai kūrimas arba apsaugotos programinės įrangos, kuri gali būti naudojama įsilaužtų pagrindinių kompiuterių atkūrimui, paskirstymas. Tai taip pat gali apimti priemonių ar programų priedų (*scripts*), praplečiančių esamų apsaugos priemonių, pavyzdžiui, naujų jungčių, skirtų pažeidžiamumo ar tinklo skaitytuvui, kodavimo technologijų naudojimą palengvinančių programų priedų ar automatinių pataisų paskirstymo mechanizmų kūrimą.

Įsilaužimo aptikimo paslaugos

Šią paslaugą teikiančios CSIRT peržiūri esamus IDS žurnalus, analizuoja ir reaguoja į visus įvykius, kurie atitinka jų nustatytą slenkstį, arba perduoda visus perspėjimus pagal iš anksto nustatytą paslaugos lygio susitarimą ar perdavimo strategiją. Įsilaužimo nustatymas ir susijusių apsaugos žurnalų analizė gali būti bauginanti užduotis: ne tik nustatant, kur aplinkoje išdėstyti jutiklius, bet ir renkant, o paskui analizuojant didelį sukauptų duomenų kiekį. Daugeliu atveju reikia specializuotų priemonių ar patirties, norint apibendrinti ir išaiškinti informaciją, siekiant nustatyti netikrus pavojaus pranešimus, užpuolimus ar įvykius tinkle, ir įgyvendinti strategijas, skirtas šiems įvykiams pašalinti ar sumažinti. Kai kurios organizacijos nusprendžia šią veiklą perduoti tiems, kas turi didesnę patirtį šios paslaugos teikimo srityje, pavyzdžiui, valdomiems apsaugos paslaugos teikėjams.

Su saugumu susijusios informacijos skleidimas

Teikiant šią paslaugą, aptarnaujami subjektai aprūpinami išsamiu ir lengvai randamu informacijos rinkiniu, padedančiu stiprinti saugumą. Ši informacija gali būti:

- CSIRT skirtos ataskaitų teikimo rekomendacijos ir kontaktinė informacija;
- perspėjimų, įspėjimų ir kitų pranešimų archyvai;
- dokumentai apie dabartinę geriausią praktiką;
- bendrosios kompiuterių ir informacijos saugumo rekomendacijos;
- politikos sritys, procedūros ir kontroliniai sąrašai;
- informacija apie programų pataisų kūrimą ir paskirstymą;
- gamintojų saitai;
- dabartiniai pranešimų apie incidentus statistiniai duomenys ir tendencijos;
- kita informacija, galinti pagerinti bendrą saugumo praktiką.

Šią informaciją gali plėtoti ir skelbti CSIRT ar kita organizacijos šalis (IT, žmogiškųjų išteklių ar ryšių su žiniasklaida skyriai). Ji gali apimti informaciją iš išorės šaltinių, tokių kaip kitos CSIRT, gamintojai ir saugumo ekspertai.

Saugumo kokybės valdymo paslaugos

Šiai kategorijai priklausančios paslaugos nėra specifinės incidentų valdymui ar, ypač, CSIRT. Tai gerai žinomos, nustatytos paslaugos, skirtos bendram organizacijos saugumui pagerinti. Turėdama įtakos patirčiai, įgytai teikiant pirmiau aprašytas reaktyviąsias ir iniciatyviąsias paslaugas, CSIRT šioms kokybės valdymo paslaugoms, kurių kitu atveju galėtų ir nebūti, gali suteikti išskirtinių galimybių. Šios paslaugos skirtos įtraukti atsiliepimus ir įgytą patirtį, pagrįstą žiniomis, gautomis reaguojant į incidentus, trūkumus ir užpuolimus. Nustatytas įprastas paslaugas (apibūdinamas toliau) papildant šia patirtimi, sudarančia saugumo kokybės valdymo proceso dalį, galima pagerinti ilgalaikes organizacijos saugumo užtikrinimo pastangas. Priklausomai nuo organizacinės struktūros ir įsipareigojimų, CSIRT gali teikti šias paslaugas arba dalyvauti didesnės organizacijos grupės veikloje.

Toliau pateiktuose aprašymuose aiškinama, kuo CSIRT kompetencija gali būti naudinga šioms kokybės valdymo paslaugoms.

Rizikos analizė

CSIRT gali padidinti rizikos analizės ir vertinimo vertę. Taip sustiprinamas organizacijos gebėjimas vertinti tikras grėsmes, praktiškai atlikti pavojaus informaciniam turtui kokybinį ir kiekybinį vertinimą bei vertinti apsaugos ir reagavimo strategijas. Atlikdama šią paslaugą, CSIRT vadovauja ir padeda naujų sistemų ir verslo procesų informacijos apsaugos rizikos analizės veiklai arba vertina grėsmes aptarnaujamų subjektų turtui ir sistemoms bei jų užpuolimo galimybes.

Verslo operacijų tęstinumo ir sutrikimo padarinių šalinimo planavimas

Remiantis buvusiais atvejais ir kylančių incidentų ar saugumo tendencijų prognozėmis, vis daugiau incidentų gali sukelti didelį verslo operacijų pablogėjimą. Todėl planuojant reikia atsižvelgti į CSIRT patirtį ir rekomendacijas, siekiant nustatyti, kaip geriau reaguoti į tokius incidentus, kad būtų užtikrinamas verslo operacijų tęstinumas. Teikdamos šią paslaugą, CSIRT grupės dalyvauja planuojant verslo tęstinumą ir sutrikimo padarinių šalinimą, taikomus įvykiams, susijusiems su grėsmėmis kompiuterių ir informacijos saugumui bei sistemų užpuolimu.

Patarimai saugumo klausimais

CSIRT gali būti naudojamos patarti ir rekomenduoti geriausią apsaugos praktiką, kad aptarnaujami subjektai galėtų vykdyti verslo operacijas. Teikdama šią paslaugą, CSIRT rengia rekomendacijas arba nustato reikalavimus naujų sistemų, tinklo įrenginių, taikomosios programinės įrangos ar visos įmonės verslo procesų pirkimui, įdiegimui ar saugojimui. Teikiant šią paslaugą, patariama ir padedama plėtoti organizacijos ar aptarnaujamų subjektų saugumo politika. Dar gali būti duodami parodymai ar patarimai teisėtvarkos ar kitoms vyriausybinėms institucijoms.

Informacijos skleidimas

CSIRT gali nustatyti, kada aptarnaujamiems subjektams reikia daugiau informacijos ir patarimų, norint geriau atitikti priimtą saugumo praktiką ir organizacijos saugumo politiką. Teikiant daugiau bendrosios saugumo informacijos aptarnaujamiems subjektams, ne tik gerinamas jų saugumo aspektų suvokimas, bet ir padedama jiems kasdienes operacijas atlikti daug saugiau. Taip galima sumažinti sėkmingų užpuolimų skaičių ir padidinti tikimybę, kad aptarnaujami subjektai aptiks užpuolimus ir praneš apie juos, taip sutrumpindami sutrikimų šalinimo laiką ir išvengdami nuostolių arba juos sumažindami.
Teikdamos šią paslaugą, CSIRT siekia galimybių padidinti informacijos skleidimą, kurdama straipsnius, plakatus, naujienų biuletenius, tinklavietes ar kitus informacijos šaltinius, paaiškinančius geriausią saugumo praktiką ir teikiančius patarimus, kokių imtis saugumo priemonių. Tai taip pat gali būti susirinkimų ir seminarų planavimas, kad aptarnaujami subjektai būtų supažindinami su naujausiomis taikomomis saugumo procedūromis ir galimomis grėsmėmis organizacijos sistemoms.

Švietimas ir mokymas

Teikiant šią paslaugą, saugumo klausimais aptarnaujami subjektai informuojami rengiant seminarus, praktinius pasitarimus, kursus ir konsultacijas. Gali būti nagrinėjamos temos, susijusios su ataskaitų teikimo gairėmis, atitinkamais reagavimo metodais, reagavimo į incidentus priemonėmis, incidentų prevencijos metodais ir kita informacija, būtina

apsaugoti nuo tinklų ir informacijos saugumo incidentų, juos nustatyti, pranešti apie juos ir į juos reaguoti.

Produkto vertinimas arba sertifikavimas

Teikdama šią paslaugą, CSIRT gali vertinti produktus, tikrindama priemones, taikomąsias programas ar kitas paslaugas, kad būtų užtikrinamas produktų saugumas ir jų atitikimas priimtinai CSIRT ar organizacijos saugumo praktikai. Peržiūrėtos priemonės ir programos gali būti atviro šaltinio ar komerciniai produktai. Ši paslauga gali būti teikiama atliekant vertinimą arba vykdant sertifikavimo programą, priklausomai nuo organizacijos ar CSIRT taikomų standartų.

A.3 Pavyzdžiai

Išgalvota CSIRT

0 žingsnis. Suprasti, kas yra CSIRT:

Suprasti, kas yra CSIRT

Pavyzdžiui, pavyzdinė CSIRT turės teikti paslaugas vidutinei įstaigai, kurioje dirba iki 200 darbuotojų. Įstaiga turi savo IT skyrių ir du filialus toje pačioje šalyje. IT sistema įmonei itin svarbi, kadangi ji naudojama vidaus ryšiams, duomenų tinklui ir visą parą bei septynias dienas per savaitę (24x7) veikiančiam elektroniniam verslui. Įstaiga turi savo tinklą ir naudojasi dviejų interneto paslaugų teikėjų (ISP) teikiama prieiga prie interneto.

- -

1 žingsnis: pradinis etapas

Pradiniame etape nauja CSIRT planuojama kaip vidinė CSIRT, teikianti paslaugas pagrindinės įmonės vietiniam IT skyriui ir darbuotojams. Ji taip pat remia ir koordinuoja su IT saugumu susijusių incidentų valdymą įvairiuose filialuose.

- -

2 žingsnis: tinkamų paslaugų pasirinkimas

Pradiniame etape nutariama, kad naujoji CSIRT daugiausia dėmesio teiks tam tikrų pagrindinių paslaugų teikimui.

Nusprendžiama, kad pasibaigus bandomajam etapui, gali būti svarstoma, ar nereikėtų papildyti paslaugų paketo, ir gali būti pridedamos tam tikros apsaugos valdymo paslaugos. Toks sprendimas priimamas remiantis bandomųjų aptarnaujamų subjektų atsiliepimais ir glaudžiai bendradarbiaujant su Kokybės užtikrinimo skyriumi.

- -

3 žingsnis: aptarnaujamų subjektų ir atitinkamų ryšio kanalų analizė

Kolektyvinis posėdis su kai kuriais pagrindiniais vadovybės ir aptarnaujamų subjektų asmenimis itin padėjo atlikti SWOT analizę. Padaryta išvada, kad būtinos šios pagrindinės paslaugos:

- Perspėjimai ir įspėjimai
- Incidentų valdymas (analizė, parama reagavimui ir reagavimo koordinavimas)
- Pranešimai

Būtina užtikrinti, kad informacijos skleidimas būtų gerai organizuotas, kad pasiektų kuo didesnę aptarnaujamų subjektų dalį. Taigi nusprendžiama, kad perspėjimai, įspėjimai ir pranešimai saugumo biuletenių forma bus skelbiami specialioje tinklavietėje ir platinami naudojant adresatų sąrašą. CSIRT palengvina pranešimų apie incidentus gavimą el. paštu, telefonu ir faksu. Kitame žingsnyje planuojamas vienodos formos el. blankas.

- -

4 žingsnis: veiklos apibrėžimas

Išgalvotos CSIRT vadovybė veiklą apibrėžė taip:
„Išgalvota CSIRT savo pagrindinės įmonės darbuotojams teikia informaciją ir padeda mažinti tinklų ir informacijos saugumo incidentų riziką, taip pat reaguoja į tokius incidentus, jiems kilus".

Šia formuluote išgalvota CSIRT aiškiai pasako, kad ji yra vidinė CSIRT, kurios pagrindinė veikla – spręsti su IT sauga susijusius klausimus.

- -

5 žingsnis: verslo plano sudarymas

Finansinis modelis
Kadangi įmonė 24 valandas per parą ir 7 dienas per savaitę užsiima el. verslu ir turi tokiu pačiu metu veikiantį IT skyrių, nuspręsta, kad darbo valandomis bus teikiamos visos paslaugos, o pasibaigus darbo dienai – budinčiojo. Paslaugos aptarnaujamiems subjektams bus teikiamos nemokamai, tačiau galimybė paslaugas teikti išoriniams klientams bus apsvarstyta bandomojo ir vertinimo etapo metu

Pajamų modelis
Pradiniame ir bandomajame etape CSIRT grupę finansuos pagrindinė įmonė. Bandomojo ir vertinimo etapo metu bus apsvarstyta papildomo finansavimo galimybė, taip pat paslaugų teikimo išorės klientams galimybė.

Organizacinis modelis
Pagrindinė organizacija yra maža įmonė, todėl pasirenkamas integruotasis modelis.
Darbo valandomis trys darbuotojai teiks pagrindines paslaugas (saugumo biuletenių platinimo ir incidentų valdymo/koordinavimo).

Įmonės IT skyriuje jau dirba tinkamos kvalifikacijos žmonės. Su šiuo skyriumi sudaromas susitarimas, kad, prireikus, CSIRT gali prašyti pagalbos tam tikrais atvejais. Be to, galima naudotis antrąja budinčių specialistų linija.
Tai bus pagrindinė CSIRT grupė, sudaryta iš keturių visą darbo dieną dirbančių narių ir penkių papildomų grupės narių. Vienas jų visuomet budi.

Darbuotojai
CSIRT grupės vadovas turi kvalifikaciją apsaugos ir 1 bei 2 lygio pagalbos teikimo srityje, taip pat dirbo funkcinio atsparumo krizių valdymo veiklos srityje. Kiti trys grupės nariai yra saugos specialistai. Pusę darbo dienos dirbantys CSIRT grupės nariai iš IT skyriaus yra įmonės infrastruktūros dalies specialistai.

- -

5 žingsnis: biuro panaudojimas ir informacijos apsaugos politika

Biuro įranga ir vieta

Atsižvelgiant į tai, kad pagrindinėje įmonėje jau taikoma pakankama fizinė apsauga, ji taip pat taikoma ir naujai CSIRT. Yra numatytas vadinamasis „gynybos kambarys“, skirtas veiksmams derinti ekstremalių situacijų atveju. Nupirktas seifas, skirtas koduotai medžiagai ir slaptiems dokumentams laikyti. Buvo įsteigta atskira telefono linija, įskaitant komutatorių, kad darbo valandomis būtų palengvintas ryšys specialia telefono linija, ir „budintis“ mobilusis telefonas, turintis tą patį numerį bei skirtas skambinti po darbo valandų.

Be to, galima naudoti esamą įrangą ir įmonės tinklavietę su CSIRT susijusiai informacijai skelbti. Įdiegta ir prižiūrima adresatų sąrašų programa, turinti ribojamos prieigos dalį bendravimui su grupės nariais ir kitomis grupėmis. Visi personalo narių kontaktiniai duomenys laikomi duomenų bazėje, spausdinta medžiaga – seife.

Reguliavimas

Kadangi CSIRT yra integruota į įmonę, turinčią informacijos apsaugos politiką, atitinkama grupės politika buvo suformuota padedant įmonės patarėjui teisės klausimais.

- -

7 žingsnis: bendradarbiavimo galimybių ieškojimas

Naudojantis ENISA apžvalga, toje pačioje šalyje greitai rastos kelios CSIRT, su kuriomis susisiekta. Surengtas neseniai pasamdyto grupės vadovo susitikimas su viena iš jų. Jis susipažino su nacionalinės CSIRT veikla ir dalyvavo susirinkime.

Šis susirinkimas buvo itin naudingas, kadangi jame pateikta darbo metodų pavyzdžių, sulaukta kelių kitų grupių paramos.

- -

8 žingsnis: verslo plano rėmimas

Nuspręsta rinkti faktus ir skaičius iš įmonės istorijos. Tai itin padeda atlikti statistinę IT apsaugos padėties apžvalgą. Įkūrus CSIRT ir jai veikiant, jie turi būti renkami toliau, kad statistiniai duomenis būtų nuolat aktualizuojami.

Susisiekta su kitomis šalies CSIRT ir pasikalbėta apie jų ekonominius modelius. Jos padėjo – parengė skaidrių su informacija apie pastarojo meto įvykius IT apsaugos incidentų srityje ir dėl incidentų patirtas išlaidas.

Šiuo išgalvotos CSIRT atveju nebuvo didelės būtinybės įtikinėti vadovybės dėl IT verslo svarbos, todėl nebuvo sunku gauti leidimą žengti pirmą žingsnį. Parengtas ekonominis modelis ir projekto planas, taip pat steigimo ir veiklos išlaidų vertinimas.

- -

9 žingsnis: proceso eigos ir veiklos bei techninių procedūrų nustatymas
Išgalvotos CSIRT tikslas – teikti pagrindines CSIRT paslaugas:

- Perspėjimus ir įspėjimus
- Pranešimus
- Incidentų valdymą

Grupė sukūrė procedūras, kurios veikia sklandžiai ir yra gerai suprantamos kiekvienam grupės nariui. Grupė taip pat pasamdė teisės specialistą, kuris užsiims įsipareigojimais ir informacijos apsaugos politika. Grupė išsirinko kelias naudingas programas ir, pasitarusi su kitomis CSIRT, rado naudingos informacijos apie veiklos aspektus.

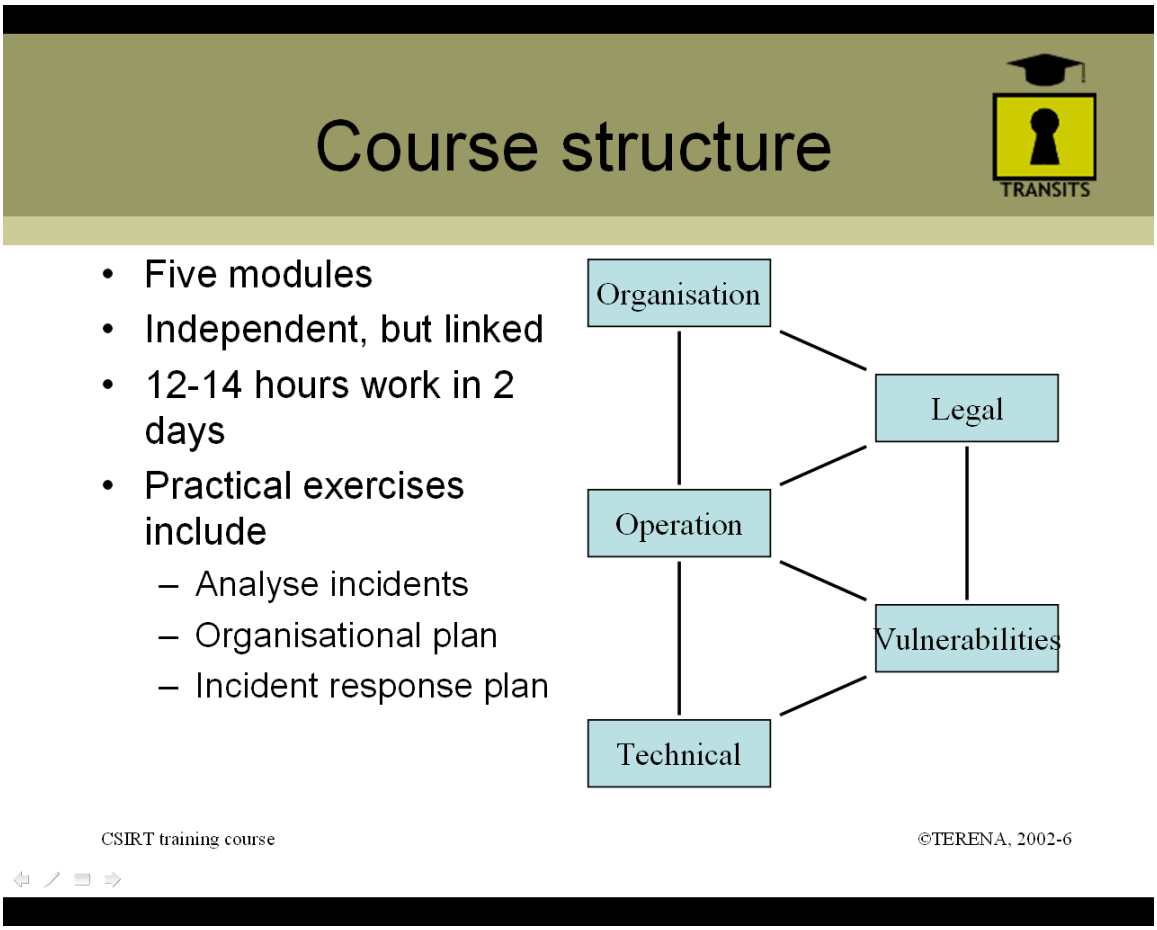
Sukurtas nuolatinis apsaugos biuletenio ir pranešimų apie incidentus šablonas. Incidentams valdyti grupė naudoja RTIR programą.
- -

10 žingsnis: darbuotojų mokymas
Išgalvota CSIRT nusprendžia visus savo techninius darbuotojus nusiųsti į būsimus TRANSITS kursus. Grupės vadovas papildomai lanko CERT/CC parengtą „Vadovavimo CSIRT“ kursą.
- -

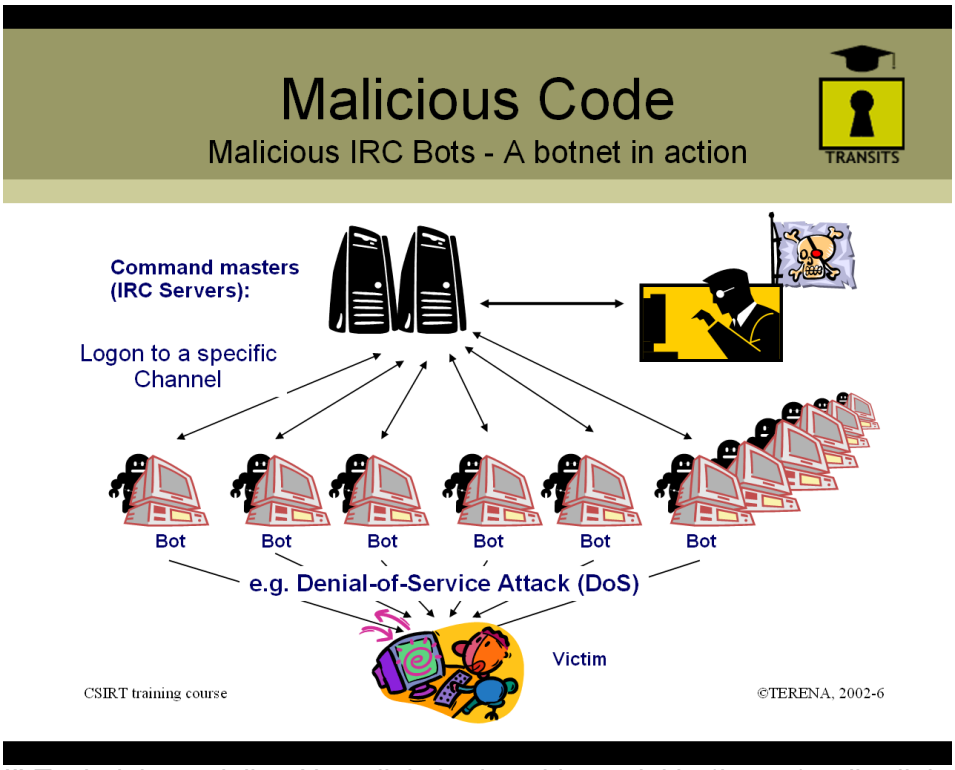
11 žingsnis: pratybos
Pirmomis veiklos savaitėmis išgalvota CSIRT pratyboms naudojo kelis netikrus atvejus (jų pavyzdžius gavo iš kitų CSIRT). Be to, grupė išleido kelis tikra aparatinės ir programinės įrangos gamintojų išplatinta informacija apie pažeidžiamumą pagrįstus saugos biuletenius, kuriuos tiksliai pritaikė aptarnaujamų subjektų poreikiams.

A.4 CSIRT kursų medžiagos pavyzdys

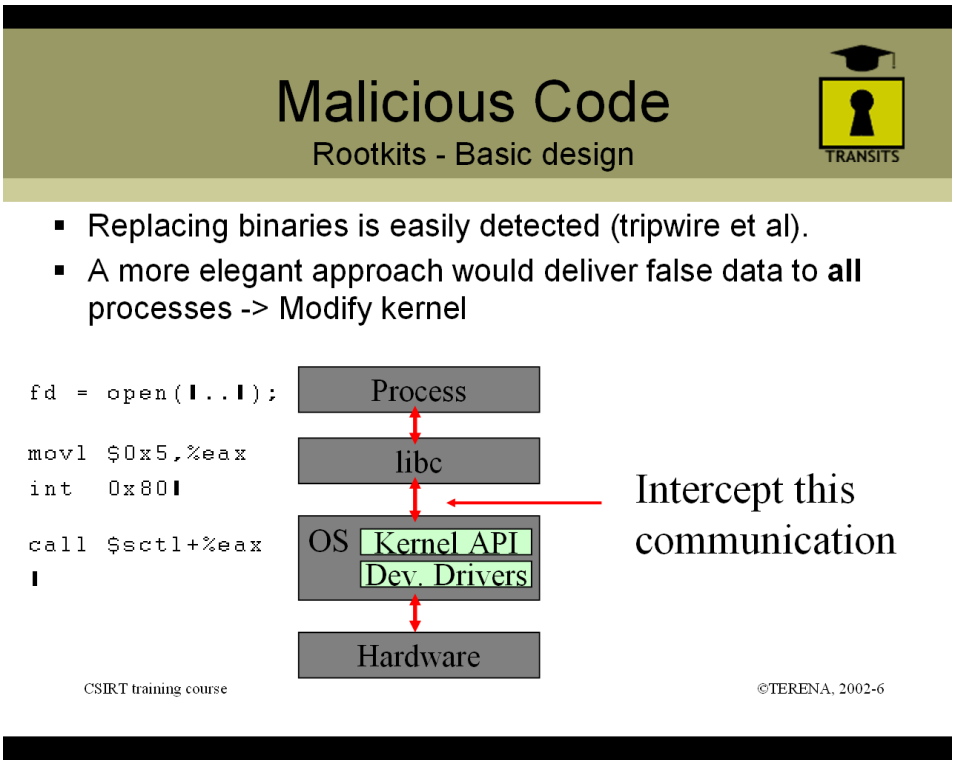
TRANSITS (Asociacijai „Terena“ maloniai leidus, http://www.terena.nl)



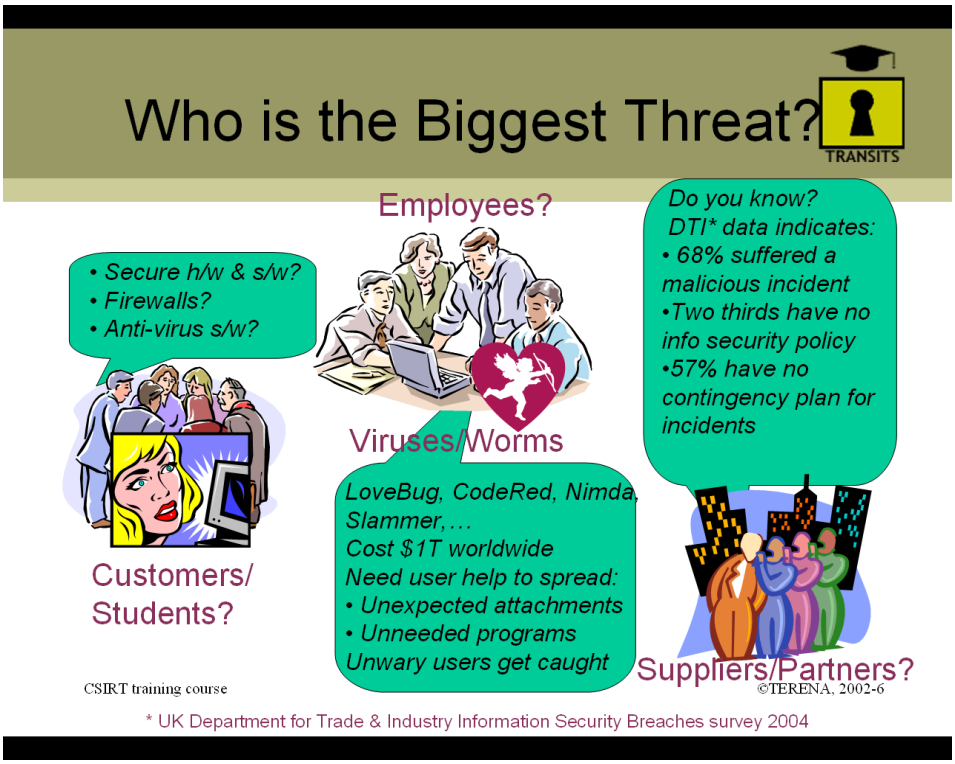
Kurso struktūros apžvalga.



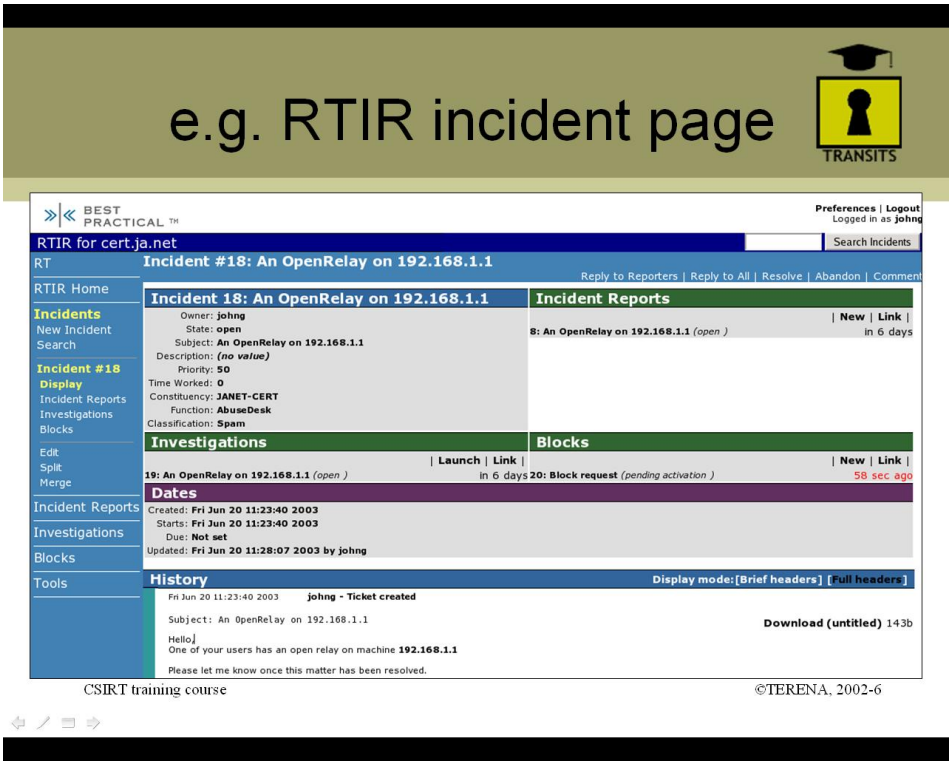
Iš Techninio modulio: „Nuotoliniu būdu valdomų tinklų (*botnet*) apibūdinimas“.



Iš Techninio modulio: „Pagrindinis *rootkit* modelis“.



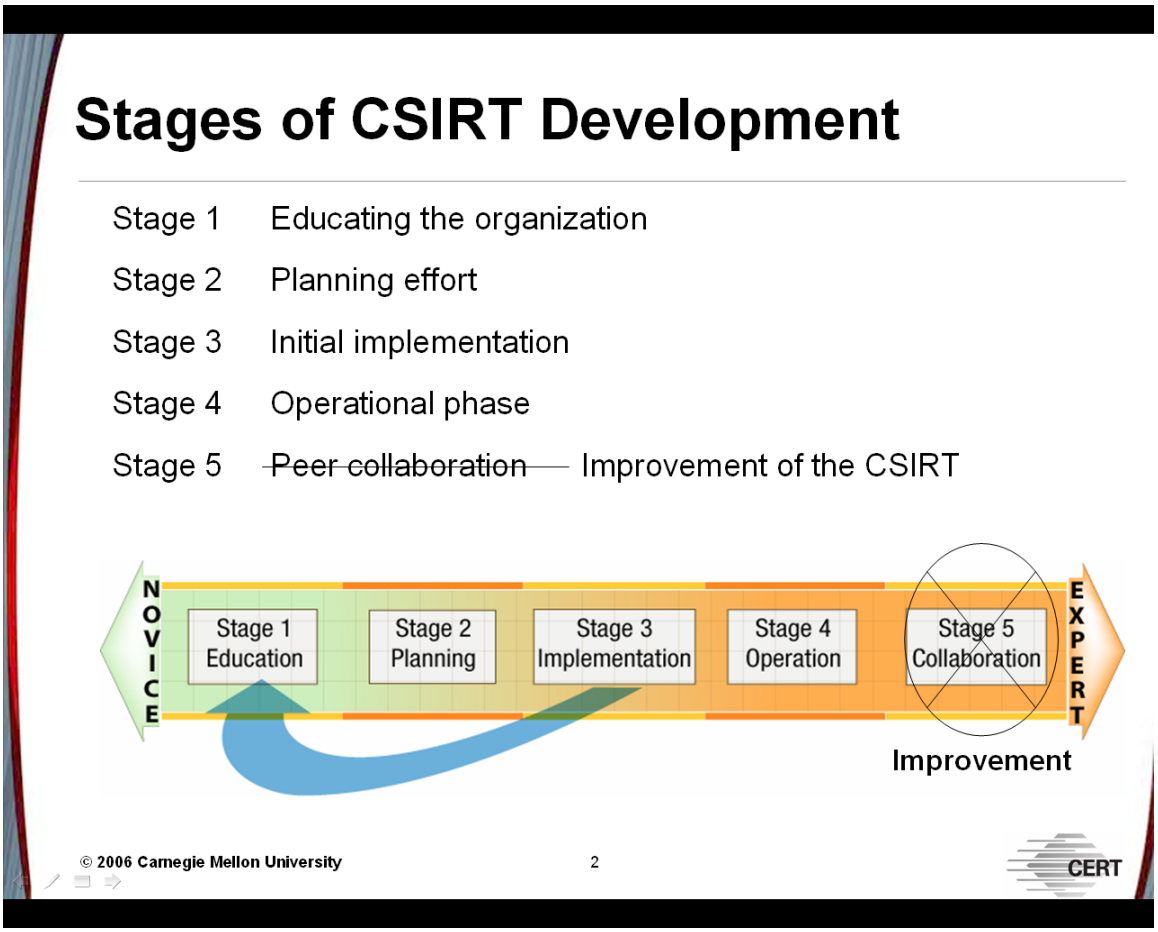
Iš Organizacinio modulio: „Kas kelia didesnę grėsmę – savas darbuotojas ar pašalinis asmuo?“



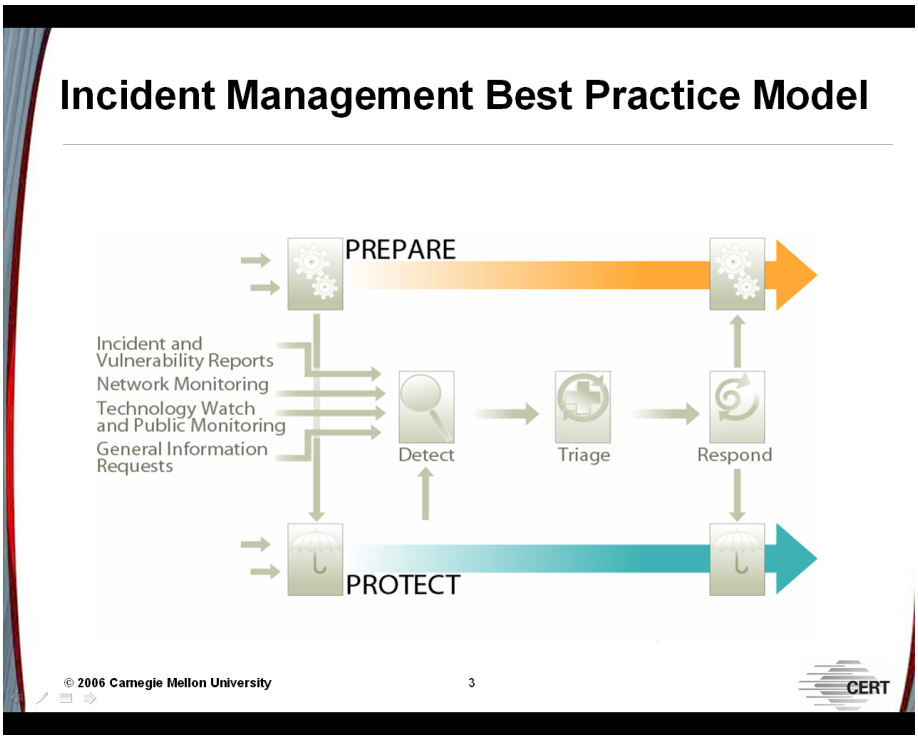
Iš „Operatyvinis sekimas“: programa „Request Tracker for Incident Response“ (RTIR).

„CSIRT grupių steigimas“ (CERT/CC maloniai leidus, http://www.cert.org)

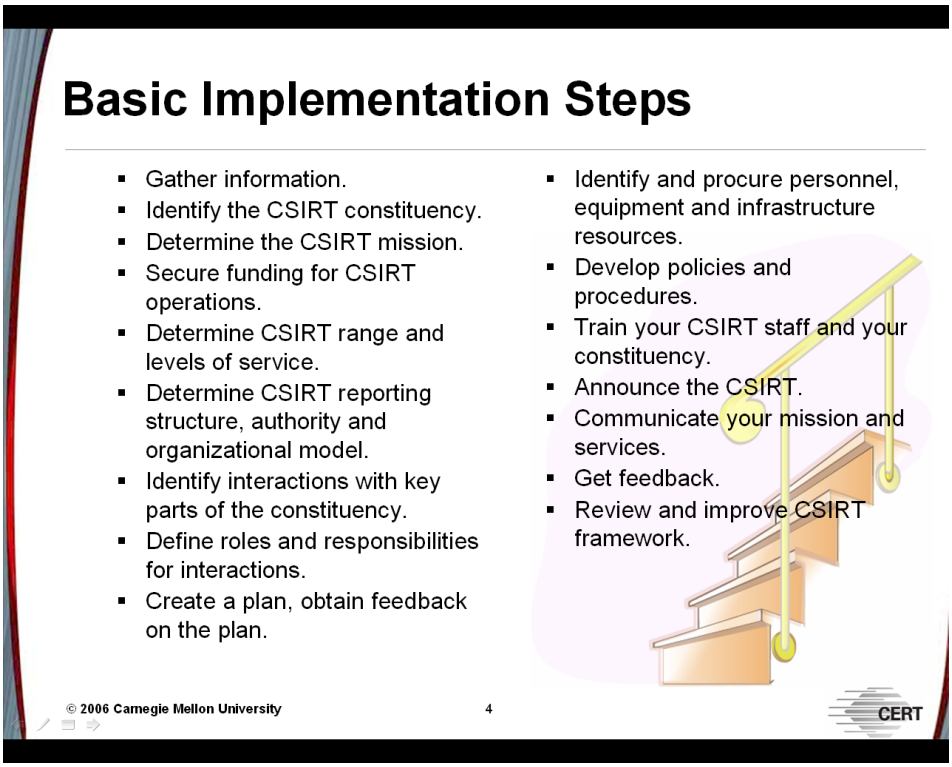
ENISA nuoširdžiai dėkoja CERT programos CSIRT plėtros grupei už leidimą naudotis jų specialistų rengimo kursų turiniu!



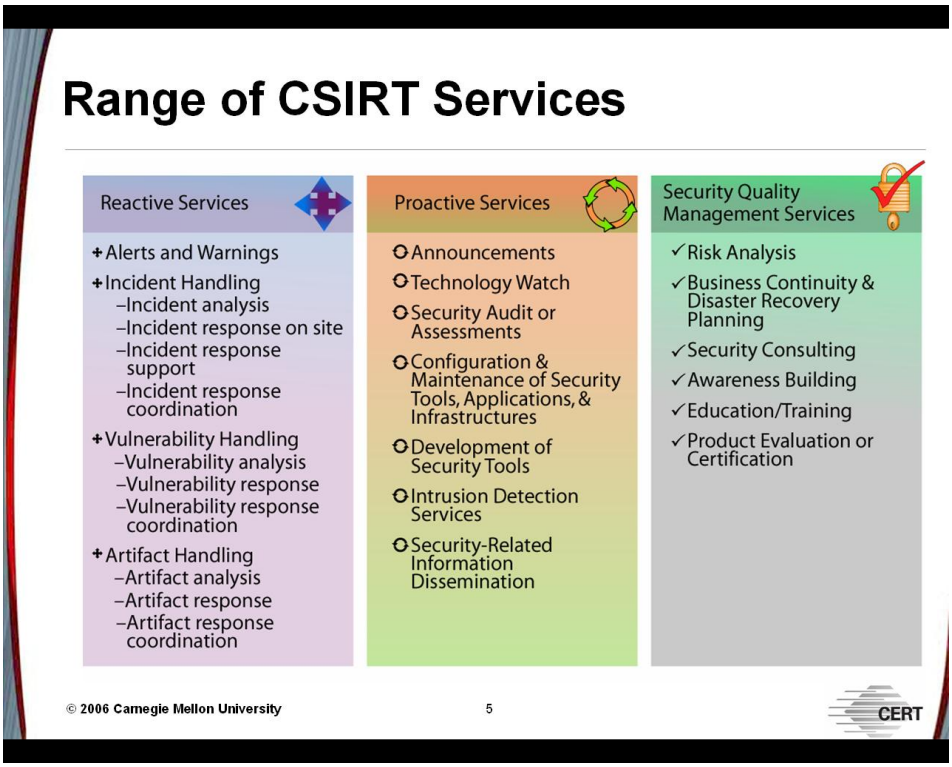
Iš *CERT/CC specialistų rengimo kurso:* „CSIRT tobulinimo etapai“.



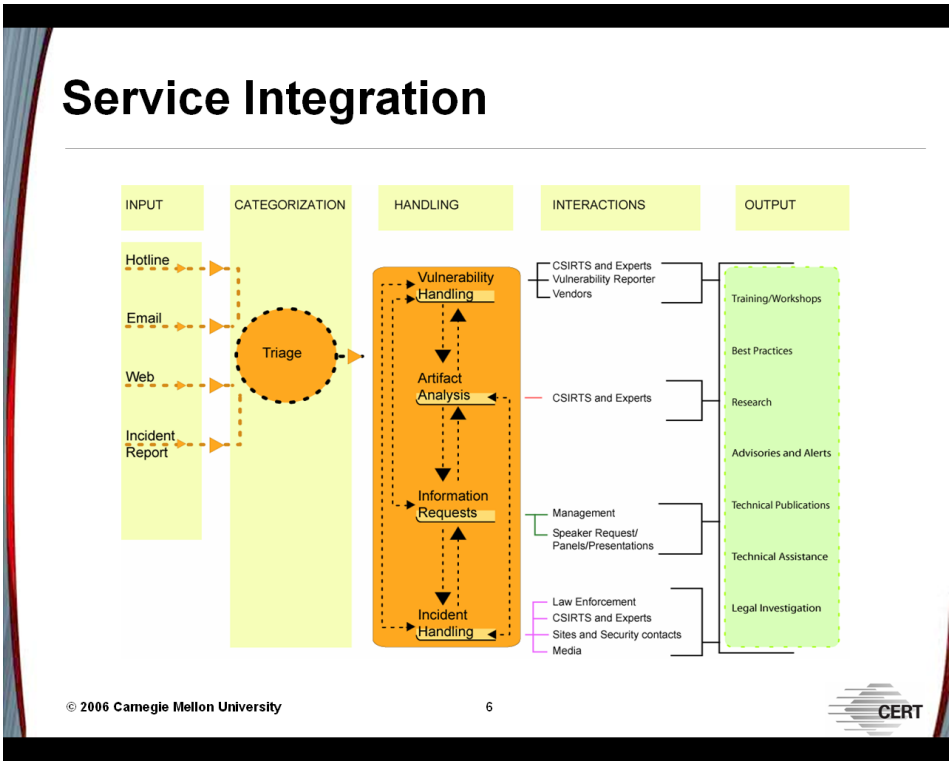
Iš *CERT/CC specialistų rengimo kurso:* „Geriausia incidentų valdymo praktika“.



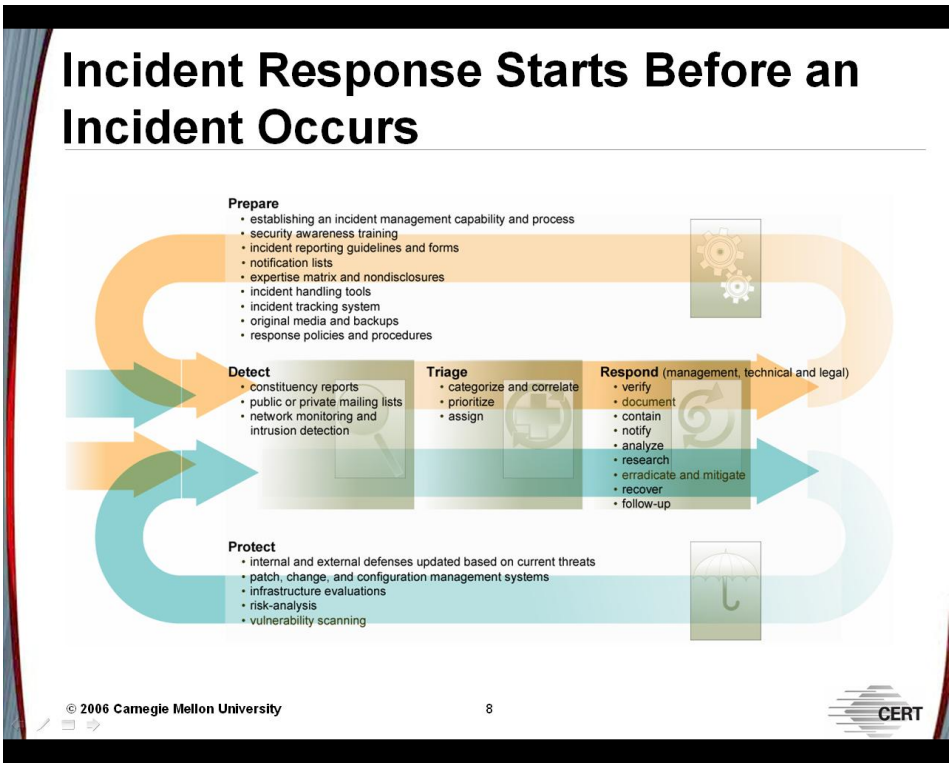
Iš *CERT/CC specialistų rengimo kurso:* „CSIRT kūrimo žingsniai“.



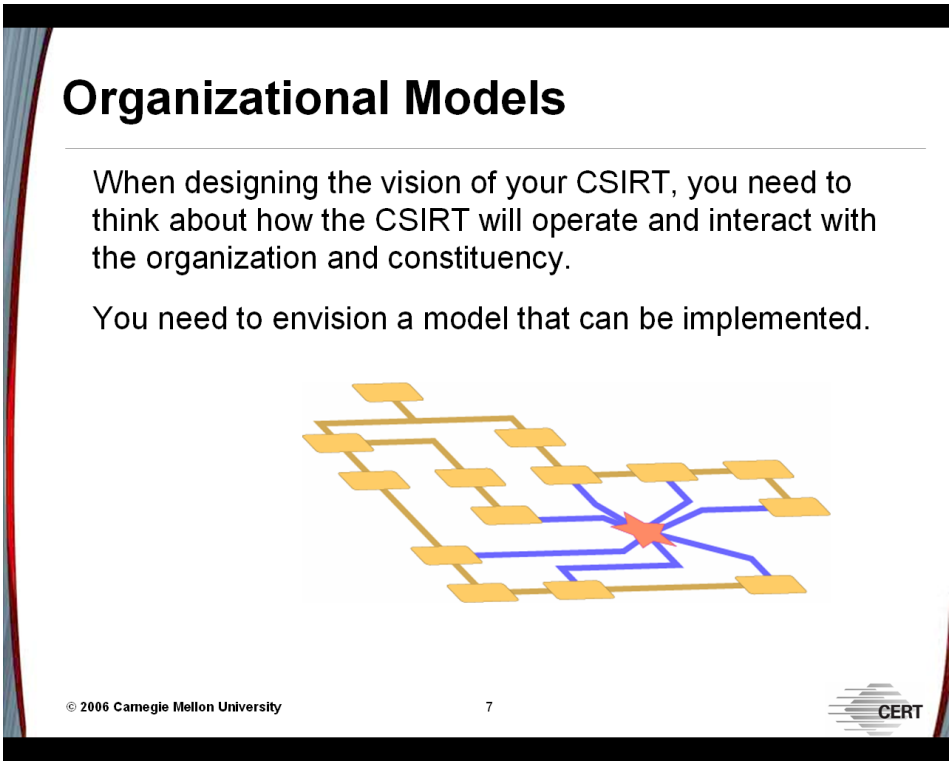
Iš *CERT/CC specialistų rengimo kurso:* „Paslaugos, kurias gali teikti CSIRT“.



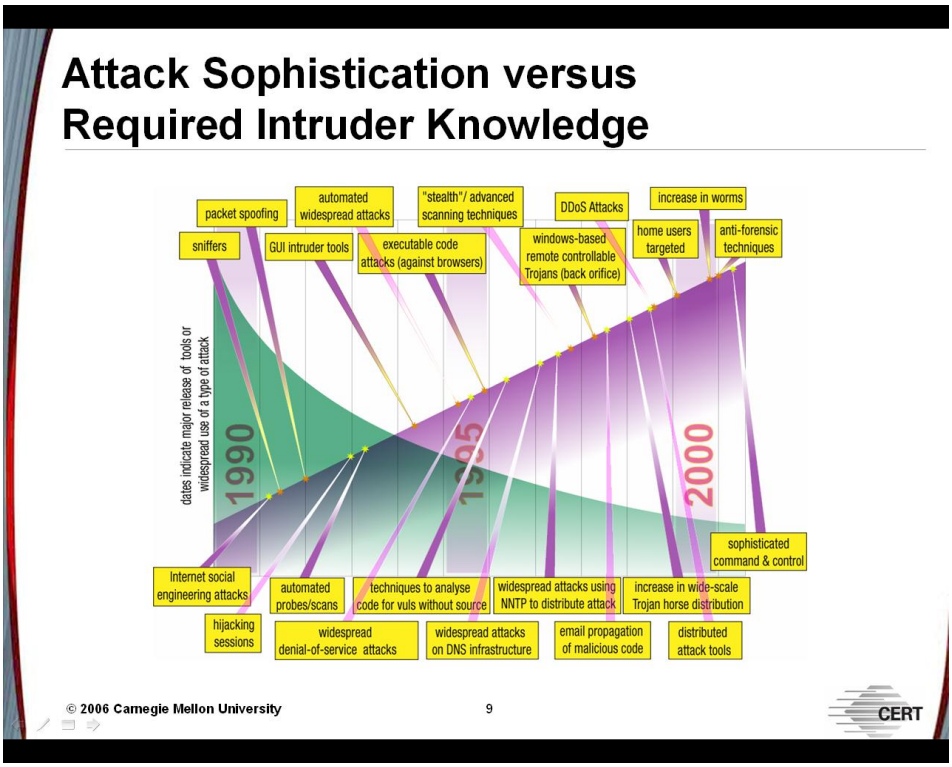
Iš *CERT/CC Specialistų rengimo kurso:* „Incidentų valdymo darbų srautas“.



Iš *CERT/CC specialistų rengimo kurso:* „Reagavimas į incidentą“.



Iš *CERT/CC specialistų rengimo kurso:* „Kaip bus organizuojama CSIRT?“.



Iš *CERT/CC specialistų rengimo kurso:* „Mažiau žinių, daugiau žalos“.