REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Udhëzim për Metodologjinë e Organizimit dhe Funksionimit të CSIRT-eve në Nivel Kombëtar

Tabela e përmbajtjes

Lista e Tabelave

Lista e figurave

Hyrje

Ky udhëzim është hartuar në zbatim të Ligjit Nr. 2/2017 “Për Sigurinë Kibernetike”, Neni 7, pika 3 dhe përshkruan procesin e krijimit të CSIRT sektorial nga perspektiva e menaxhimit të skuadrës, menaxhimit të proceseve të punës dhe perspektiva teknike.

Rrjetet e komunikimit dhe sistemet e informacionit janë bërë një faktor thelbësor në zhvillimin ekonomik dhe social. Siguria e rrjeteve të komunikimit dhe sistemeve të informacionit, e në veçanti disponueshmëria e tyre, përbëjnë një shqetësim në rritje për shoqërinë. Kjo vjen si pasojë e rrezikut në rritje të problemeve që mund të ndodhin në sistemet e informacionit, për shkak të kompleksitetit të sistemit, aksidenteve, gabimeve dhe sulmeve ndaj infrastrukturave fizike që ofrojnë shërbime esenciale për qytetarët.

Udhëzimi shërben si një metodologji pune për ngritjen dhe organizimin e CSIRT-eve nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, sipas listës që i bashkëlidhet VKM nr. 222 datë 26.04.2018 "Për miratimin e Listës së Infrastrukturave Kritike të Informacionit dhe të Listës së Infrastrukturave të Rëndësishme të Informacionit".

Qëllimi

Përcaktimi i rregullave për krijimin dhe funksionimin e CSIRT-eve në nivel kombëtar për mbrojtjen dhe rritjen e niveleve të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit.

Objektivat

1. Përcaktimi i rregullave / detyrave për fuksionimin e CSIRT-it kombëtar dhe sektorial.
2. Sigurimi dhe ruajtja e rrjeteve të komunikimit dhe sistemeve të informacionit për të siguruar disponueshmërinë, integritetin dhe konfidencialitetin, pranë OIKI dhe OIRI.
3. Krijimi i një rrjeti bashkëpunimi sektorial për rritjen e nivelit të sigurisë.

Përkufizime

"CSIRT Kombëtar" - sipas nenit 5, të ligjit nr 2/2017 "Për sigurinë kibernetike"

"CSIRT sektorial" - është ekipi/ personi përgjegjës ndaj Incidenteve të Sigurisë Kibernetike, në strukturën e një operatori që administron ***infrastruktura kritike dhe të rëndësishme të informacionit.*** CSIRT-et sektoriale, trajtohen sipas emërtesës në aneksin bashkëlidhur VKM nr. 222 datë 26.04.2018 "Për miratimin e Listës së Infrastrukturave Kritike të Informacionit dhe të Listës së Infrastrukturave të Rëndësishme të Informacionit".

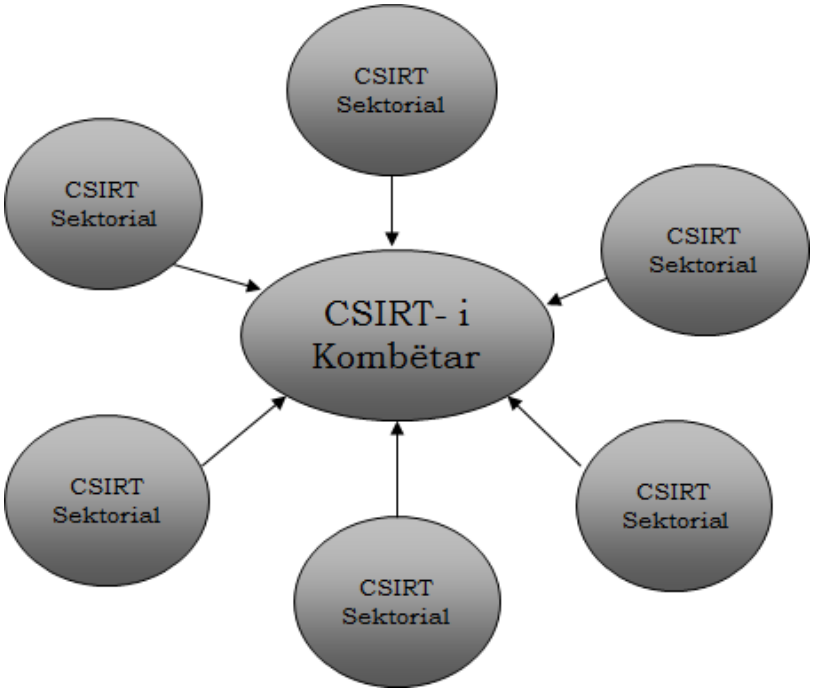


Figura 1 Diagrama e paraqitjes dhe raportimit të CSIRT-eve

1. Menaxhimi i ciklit të jetës së CSIRT-it

Përpara ngritjes së një CSIRT-i duhen konsideruar disa faktorë. Organizatat ndërkombëtare si ENISA dhe FIRST rekomandojnë të konsiderohet metoda Plan – Do – Check – Act (PDCA) për të planifikuar siç duhet krijimin e skuadrës dhe për të lejuar përmirësimin e vazhdueshëm të strukturës.

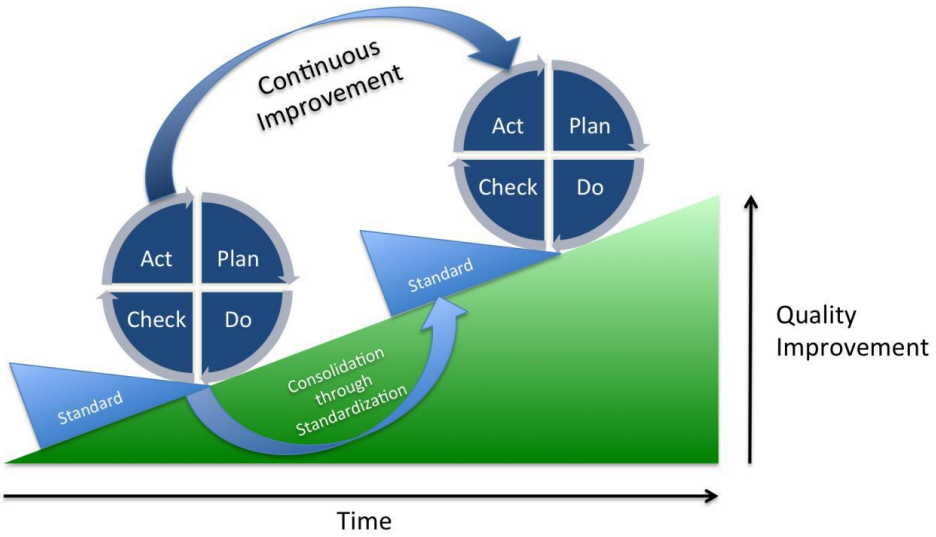


Figura 2 Paraqitja e ciklit PDCA

Vendimmarrësit e lartë duhet të konsiderojnë elementët e mëposhtëm, sipas ciklit të paraqitur më sipër:

PLAN

Krijimi i kuadrit të përgjithshëm të CSIRT-it

- Kjo çështje do të përshkruhet në detaje në kapitullin e rradhës dhe në Aneksin: "Formulari i kuadrit të përgjithshëm të CSIRT"

Krijimi i buxhetit

- Përpiloni një plan buxheti disa vjeçar, ku të ndahen qartë kostot operacionale dhe kostot e investimit
- Mos shtoni zëra të panevojshëm në buxhet dhe përpiquni të përfshini çdo zë të domosdoshëm për veprimtarinë e përditshme të ekipit

Krijoni një plan pune të qartë

- Plani i punës duhet të reflektojë qëllimet e CSIRT-it brenda organizatës dhe të tregojë se si qëllimet lidhen me buxhetin

DO

Implementoni planin e punës

- Siç përshkruhet në kapitullin 4 dhe 5
  - Krijoni një pamje të përgjithshme të burimeve të informacionit
  - Krijoni politikën për Trajtimin e Incidenteve
  - Krijoni politikën për Shkëmbimin dhe trajtimin e informacionit
  - Komunikoni ekzistencën e CSIRT-it (Bëjeni të ditur për palët e tjera)
  - Krijoni rrjetin e besimit, duke ndjekur konferenca dhe seminare
  - Praktikoni këtë proces në mënyrë të vazhdueshme
- Realizoni veprimet e përditshme të CSIRT-it për trajtimin e incidenteve (siç përshkruhet në kapitullin përkatës) dhe shërbimet themelore (siç përshkruhen në kapitullin 6)

CHECK

Analizoni performancën e skuadrës

- Fokusohuni në proceset dhe detyrat më të rëndësishme
  - Ato që realizoni më shpesh
  - Ato që kërkojnë realizim inkonsistent
  - Ato që kërkojnë kontrollin tuaj shtesë për t'u përmirësuar
- Përcaktoni objektiva të matshëm
- Përfshini të gjithë anëtarët e skuadrës
  - Përfshirja e anëtarëve të skuadrës ndan angazhimin në realizimin e detyrave
  - Evidentoni çfarë kanë realizuar me sukses dhe ku ka nevojë për përmirësim
  - Punoni me departamentin Quality Assurance (Departamenti I Sigurmit të Cilësisë) nëse ekziston në organizatën tuaj
  - Konsideroni përfshirjen e konsulentëve të jashtëm
- Realizoni intervista me punonjësit e tjerë të organizatës
  - Çfarë ka realizuar me sukses CSIRT?
  - Cilat janë fushat që ka nevojë për përmirësim?

- Menaxhoni cilësinë
  - A realizohet puna sipas proceseve dhe standardeve?
  - A dokumentohet puna?
  - A janë të gjithë anëtarët e ekipit në dijeni për vendndodhjen e dokumentacionit?
  - A mbahen minutat e takimeve për t'iu referuar në të ardhmen sipas nevojave të CSIRT-it?
  - Si realizohet bashkëpunimi brenda skuadrës?
  - A ruhen evidenca për ndjekjen e trajnimeve, konferencave dhe seminareve?

ACT

Përcaktoni çfarë ka nevojë për përmirësim

- Pas rezultateve të fazës “CHECK”, mund të realizohen përmirësimet sipas fushave ku janë evidentuar
- Ndërkohë që shërbimet e skuadrës maturohen, mund të nevojiten shërbime shtesë, siç përshkruhen në kapitullin 6
- Filloni të planifikoni një tjetër fazë “PLAN” për të implementuar përmirësimet, dhe ndiqni të gjitha fazat deri në fazën “ACT”.

Pas krjimit të skuadrës së CSIRT-it, rekomandohet që cikli “PDCA” të kryhet një herë në vit, për t’u siguruar që kërkesat e CSIRT-it reflekohen në buxhet dhe janë në harmoni me kërkesat e vetë organizatës.

1.1 Matja dhe përmirësimi i nivelit të maturitetit të CSIRT-it

Një mënyrë për të përzgjedhur shërbimet që do të ofrojë CSIRT-i është duke matur nivelin e maturitetit të skuadrës, të cilat variojnë nga shërbimet reaktive deri në implementimn e shërbimeve proaktive dhe menaxhimit të cilësisë.

Nivelet e maturitetit së bashku me përshkrimin për secilin nivel.

Niveli i maturitetit	Përshkrimi
1. Fillestar	CSIRT-i ekziston si pikë kontakti për koordinimin dhe zgjidhjen e incidenteve. Gjithashtu janë krijuar rregulloret dhe politikat për koordinimin me autoritetet e tjera përgjegjëse.
2. Bazik	Përveç cilësive të nivelit të parë, në këtë nivel CSIRT-i ka të implementuar një proces për trajtimin e kërcënimeve të reja. Për raportimin e incidenteve përdoret një sistem i dedikuar, si psh RTIR.
3. Aktiv	Përveç cilësive të nivelit të dytë, në këtë nivel CSIRT-i ka të implementuar tools-e për të analizuar kërcënimet dhe ekzistojnë procedura për klasifikimin dhe shkëmbimin e informacionit.

4. Proaktiv	Përveç cilësive të nivelit të tretë, në këtë nivel CSIRT-i realizon rregullisht kontrolle për të ruajtur statusin e sigurisë dhe ka planifikuar trajnimin e vazhdueshëm të anëtarëve të ekipit.
5. I avancuar	Përveç cilësive të nivelit të katërt, në këtë nivel CSIRT-i monitoron në kohë reale incidentet dhe kërcënimet. Udhëzimet për kërcënimet e reja dhe parandalimin e incidenteve hartohen dhe ndahen brenda dhe jashtë organizatës me qëllim rritjen e ndërgjegjësimit.

Nivelet e maturimit të CSIRT-it i referohen pesë shtyllave të funksionmit të CSIRT:

Krijimi
Plani i punës dhe identifikimi i kufizimeve ligjore

Organizimi
Misioni dhe struktura të tjera të brendshme organizative brenda organizatës, dhe koordinimi me CSIRT-et e tjera

Faktori human
Stafi i ekipit, struktura, ekspertiza, kodi i sjelljes dhe mundësitë për trajnim

Tools-et
Çdo gjë që nevojitet për të kryer detyrat e dhëna

Proceset
Për trajtimin e kërcënimeve dhe incidenteve ose ndërveprimin me mediat

Trusted Introducer ka zhvilluar një standard për maturitetin e CSIRT të ndarë në tre nivele (Trusted Introducer process: <https://www.trusted-introducer.org/processes/overview.html>

1. Listimi
2. Akreditimi
3. Certifikimi

1.2 Vetëvlerësimi i maturitetit

Maturiteti i CSIRT mund të vlerësohet nga vetë anëtarët e ekipit online në njërin prej burimeve të mëposhtme:

- GCCS dhe NCSC-NL[1].
- ENISA[2].

2. Kuadri i përgjithshëm i CSIRT

Kuadri i përgjithshëm i CSIRT shpjegon në detaje çfarë bën CSIRT, mbi cilat burime vepron dhe cili është target grupi i shërbimeve që ai ofron. Edhe pse CSIRT-et veprojnë në fusha dhe ambjente të ndryshme, elementët përbërës që nevojiten për krijimin e tyre janë të njëjtë. Një formular për këta elementë gjendet në Aneksin A.

Çfarë është CSIRT?

CSIRT është ekipi i ekspertëve të sigurisë kibernetike, përgjegjësia kryesore e të cilëve është ti përgjigjen incidenteve të sigurisë kibernetike. Ekipi i CSIRT siguron shërbimet e nevojshme për ti trajtuar incidentet dhe për të rikthyer sistemin e prekur në gjendje pune.

Për të minimizuar rreziqet kibernetike, shumica e CSIRT-eve mund të ofrojnë shërbime parandaluese dhe trajnuese në mjedisin ku veprojnë. Ata ofrojnë këshilla mbi dobësitë e evidentuara në software-t dhe hardware-t që përdoren, si dhe informojnë përdoruesit për kërcënimet e ndryshme, dhe përditësimet që i duhen bërë pajisjeve dhe sistemeve rast pas rasti.

2.1 Përfitimet e ngritjes së CSIRT

Një ekip i dedikuar për përgjigje ndaj incidenteve të sigurisë kibernetike ndihmon organizatën për të zbutur dhe parandaluar incidentet potenciale, si dhe mbron asetet e saj më të vlefshme.

Të tjera përfitime të mundshme janë:

[1] <https://check.ncsc.nl/>
[2] <https://www.enisa.europa.eu/topics/csirts-in-europe/csirtcapabilities/csirt-maturity/csirt-maturity-self-assessment-survey>

- √ Koordinim i centralizuar për çështjet e sigurisë brenda organizatës, nëpërmjet caktimit të një pike qendrore kontakti brenda CSIRT për komunikim me CSIRT Kombëtar.
- √ Trajtim dhe reagim i centralizuar dhe i specializuar ndaj incidenteve të sigurisë.
- √ Ofrim i ekspertizës ndaj punonjësve të organizatës në çdo kohë me qëllim rikuperimin pas incidenteve të sigurisë.
- √ Ruajtja e evidencave kompjuterike në rast se ndaj organizatës ngihen padi gjyqësore.
- √ Ndjekja e zhvillimeve në fushën e sigurisë dhe integrimi i tyre brenda organizatës.
- √ Nxitja e bashkëpunimit me punonjësit e tjerë të organizatës dhe rritja e ndërgjegjësimit për çështjet e sigurisë për të gjithë punonjësit e saj.
- √ Përfitimi i informacioneve për sulme kibernetike në *real time* nga homologët me qëllim marrjen e masave për parandalimin e incidenteve kibernetike.

2.2 Kërkesat funksionale të CSIRT-eve:

1. CSIRT-et duhet të sigurojnë një nivel të lartë të disponueshmërisë së shërbimeve të tyre të komunikimit dhe të disponojnë disa mjete për t'u kontaktuar dhe për të kontaktuar me të tjerët në të çdo kohë.
2. Sistemet e informacionit që administron CSIRT duhet të jenë të vendosura në zona të sigurta fizikisht.
3. CSIRT-et duhet të mundësojnë komunikimin nëpërmjet një platforme ndërveprimi për menaxhimin dhe drejtimin e kërkesave, në mënyrë që të lehtësohet menaxhimi i trajtimit të incidenteve.
4. CSIRT-et duhet të kenë staf të mjaftueshëm dhe të kualifikuar, për të siguruar disponueshmërinë në çdo kohë.
5. CSIRT-et duhet të mbështeten në një infrastrukturë, vazhdimësia e së cilës duhet të jetë e garantuar.
6. CSIRT-et duhet të krijojnë mundësitë për të bashkëpunuar me rrjetet ndërkombëtare homologe, për të garantuar një standard me të lartë të trajtimit dhe zgjidhjes së incidenteve kibernetike.

3. Aftësitë bazë të CSIRT-eve

Sipas ENISA, aftësitë bazë që duhet të zotërojë një CSIRT ndahen në 4 kategori:

1. Shërbimet që ofron CSIRT
2. Kompetencat dhe përgjegjësitë e CSIRT
3. Aftësitë operacionale të ekipit të CSIRT
4. Shpërndarja e informacionit

3.1 Shërbimet që ofron CSIRT

Portofoli i shërbimeve që ofron një CSIRT për organizatën

Shërbime Reaktive	**Shërbime proaktive**	**Trajtimi i artifakteve**
• **Alertet dhe paralajmërimet** • **Trajtimi i incidenteve** • **Analiza e incidenteve** • **Suport gjatë përgjigjes ndaj incidenteve** • **Koordinim gjatë përgjigjes ndaj incidenteve** • Përgjigje e incidentit on site • Trajtimi i vulnerabiliteteve • Analiza e vulnerabiliteteve • Përgjigje ndaj vulnerabiliteteve	• **Lajmërime** • Auditime dhe vlerësime sigurie • Konfigurime dhe mirëmbajtja e sigurisë • Zhvillimi i tool-eve të sigurisë • Shërbime Intrusion Detection • Shpërndarja e informacioneve të vlefshme për rritjen e sigurisë	• Analiza e artifakteve • Përgjigje e aktifakteve • Koordinim për përgjigje ndaj artifakteve **Menaxhimi i Cilësisë së Sigurisë** • Analiza e riskut • Business Continuity dhe Disaster Recovery • Konsulencë sigurie • Ndërgjegjësim • Edukim / Trajnim

Tabela 1 Shërbimet e CSIRT sipas CERT/CC

Shërbimet proaktive synojnë parandalimin e incidenteve përmes ndërgjegjësimit dhe trajnimit, ndërsa shërbimet reaktive synojnë trajtimin e incidenteve dhe minimizimin e dëmit.

Trajtimi i artifakteve përmban analizën e çdo skedari ose objekti të gjetur në sistemet e organizatës të mund të përfshihet në veprime dashakeqe, si mbetjet pas sulmit të një virusi, trojani etj.
Gjithashtu këtu përfshihet trajtimi dhe shpërndarja e informacionit tek palët e treta, për të parandaluar përhapjen e mëtejshme të malware-ve dhe zbutjen e rreziqeve.

Shërbimet e menaxhimit të cilësisë së sigurisë janë shërbime me qëllime afatgjata dhe përfshijnë masa këshilluese dhe edukative.

Nga lista e mësipërme e shërbimeve, Trajtimi i incidenteve dhe analiza e incidenteve janë shërbimi kryesor e i detyrueshëm për tu kryer nga ekipet e CSIRT. Për më tepër, organizatat ndërkombëtare rekomandojnë që paralajmërimet të ofrohen në mënyrë proaktive dhe reaktive. Shpërndarja e informacioneve të sigurisë përmirëson funksionimin

e ekipit dhe lehtëson ndërtimin e besimit për aftësitë e tij përballë organizatës ku është ngritur.

Menaxhimi i incidenteve dhe paralajmërimet janë shërbime që CSIRT duhet ti kryejë vetë, por mund që edhe ti transferojë disa nga shërbimet më pak emergjente afatmesme dhe afatgjata.

Për funksionimin e brendshëm të një CSIRT duhet të zbatohen shërbime dhe masa të tjera. Në përgjithësi është e nevojshme që një ekip në çdo kohë të jetë në dijeni për situatën e sigurisë në organizatën ku vepron, dhe në internet në përgjithësi. Të gjitha shërbimet e tjera nga lista e mësipërme konsiderohen në mënyrë parimore opsionale dhe ofrimi i tyre varet nga nevojat e organizatës.

Shumica e CSIRT-eve ofrojnë fillimisht shërbimet e ofrimit të "Alerteve dhe Paralajmërimeve", bëjnë "Lajmërimet", dhe sigurojnë "Trajtim Incidentesh" për organizatën e tyre. Këto shërbime bazë i japin një profil të mirë organizatës dhe konsiderohen vlerë e shtuar për të.

Një praktikë e mirë është ofrimi i një grupi të vogël shërbimesh, në formën e një organizimi pilot, dhe më pas shtimi i shërbimeve sipas nevojave të organizatës dhe historikut të sulmeve të ndodhura.

Pasi keni kuptuar përfitimet e ekzistencës së CSIRT dhe llojet e shërbimeve që mund të ofrojë ekipi për organizatën, hapi i rradhës është ngritja e CSIRT duke konsideruar:

- Përcaktoni mënyrën e komunikimit me pjesën tjetër të organizatës
- Përcaktoni në mënyrë të qartë misionin e CSIRT
- Përcaktoni një projekt realist dhe plan zbatimi me objektiva të realizueshëm
- Përcaktoni shërbimet që do realizojë CSIRT
- Përcaktoni strukturën organizative të CSIRT
- Përcaktoni politikën e Sigurisë së Informacionit
- Punësoni stafin e duhur
- Kërkoni bashkëpunimin e CSIRT-eve të tjera brenda sektorit tuaj

Secila prej këtyre çështjeve, shpjegohet në detaje më poshtë.

Mënyra e komunikimit me pjesën tjetër të ekipit të organizatës

Siç është thënë më sipër, është shumë e rëndësishme të njihni nevojat e organizatës, si dhe strategjinë e komunikimit të organizatës, duke përdorur kanalet më të përshtatshme të komunikimit.

CSIRT-et operojnë duke përdorur një grup kanalesh komunikimi. Më poshtë listohen më të përdorshmit dhe më të rëndësishmit për një organizatë:

- Website publik
- Zonë private e website-t të organizatës që kërkon anëtarësim sipas kritereve të caktuara
- Web-form për të raportuar incidentin
- Listat e emaileve
- E-mail të personalizuar rast pas rasti
- Telefon / faks
- SMS
- Raporte mujore dhe / ose vjetore

Informacioni duhet të shpërndahet në mënyrë të sigurtë, për shembull nëse përdoret komunikimi me e-mail, ky i fundit duhet të nënshkruhet në mënyrë digjitale me PGP. Të dhënat sensitive kur shpërndahen me e-mail, duhet të dërgohen gjithmonë të enkriptuara.

3. 2 Kompetencat dhe përgjegjësitë e CSIRT

Mandati / korniza që mbulon kompetencat dhe përgjegjësitë që ka CSIRT

Pas analizimit të nevojave të organizatës duhet përcaktuar misioni i CSIRT. Deklarata e misionit të CSIRT-it përshkruan funksionin themelor të organizatës për mjedisin ku vepron, në termat e produkteve dhe/ose shërbimeve që ofron. Gjithashtu misioni shërben për të përcaktuar funksionet e CSIRT dhe për të bërë të ditur ekzistencën e tij.

Një praktikë e mirë është përcaktimi në mënyrë kompakte e deklaratës së misionit, jo në prizëm të ngushtë, për të siguruar përputhshmërinë afatgjatë me veprimtarinë e CSIRT – it.

Më poshtë mund të gjeni një shembull për deklaratën e misionit të CSIRT:

Shembull 1

<Emri i CSIRT> siguron informacion dhe asistencë për <përbërësit e tij> në zbatimin e masave proaktive për të zvogëluar rreziqet e incidenteve të sigurisë si dhe përgjigjen ndaj incidenteve kur ato ndodhin.

Shembull 2

Të ofrojë mbështjetje për <Organizatën> për parandalim dhe përgjigje ndaj incidenteve të sigurisë.

Roli dhe përgjegjësitë e CSIRT-it duhet tu komunikohen në mënyrë të qartë të gjithë aktorëve relevantë të tjerë të industrisë ku vepron ekipi. Komunikimi i misionit të secilit CSIRT për homologët është i rëndësishëm për të shmangur konfuzionet dhe vonesat në shpërndarjen e informacionit.

Detyrat e CSIRT-eve sektoriale

1. Monitoron sistemet e infrastrukturave kritike dhe/apo të rëndësishme të informacionit mbi incidente dhe/apo sulme të mundshme kibernetike
2. Siguron back up të të dhënave të sistemeve që disponon.
3. Kontrollon dhe menaxhon incidentet kibernetike.
4. Identifikon dhe kategorizon incidentet kibernetike.
5. Vlerëson shtrirjen e incidentit dhe dëmin e shkaktuar.
6. Heton në kohë dhe vlerëson impaktin e incidentit.
7. Njofton në kohë për incidentet, që kanë impakt tek administratorët e OIKI/OIRI.
8. Siguron analizë dinamike të rrezikut dhe incidentit dhe realizon kontroll për përmbajtjen e tij.
9. Mban dhe ruan kronologjinë e të gjitha provave të incidentit, konform legjislacionit në fuqi për ruajtjen e konfidencialitetit.
10. Njofton AKCESK menjëherë pasi identifikon incidentin.
11. Ndjek me rigorozitet masat paralajmëruese të CSIRT kombëtar dhe/ose njofton AKCESK në rastin e zgjidhjes së shpejtë të incidentit.
12. Përgatit dhe dërgon pranë CSIRT kombëtar raportet e incidenteve, sipas formatit të miratuar nga AKCESK.
13. Parandalon incidente të ngjashme në të ardhmen duke marrë masa parandaluese.
14. Rikuperon të dhënat dhe kthen në normalitet sistemin e prekur brenda kohës së përcaktuar sipas rregullores për klasifikimin e incidentit, të miratuar nga AKCESK.
15. Duhet të sigurojë rritjen e kapaciteteve të stafit, nëpërmjet trajnimeve dhe certifikimeve periodike.

Detyrat e CSIRT-it Kombëtar

1. CSIRT-i kombëtar organizon dhe koordinon punën me të gjithë operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit
2. CSIRT-i kombëtar mbledh të paktën një herë në tre muaj CSIRT-et sektoriale, me qëllim evidentimin e problematikave të ndryshme të fushës dhe rritjen e bashkëpunimit.
3. Menaxhon dhe trajton çdo kërkesë të paraqitur nga CSIRT-et sektoriale në lidhje me incidentet kibernetike të mundshme.
4. Jep asistencë në kohë reale pranë CSIRT-eve sektoriale, sipas kërkesave të tyre.
5. Siguron paralajmërim të hershëm dhe shpërndan informacionin e nevojshëm për marrjen e masave parandaluese, tek operatorët në lidhje me rreziqet dhe incidentet kibernetike.
6. Kërkon raporte të detajuara nga CSIRT-et sektoriale, për çdo procedurë incidenti kibernetik.
7. Përveç rolit si CSIRT Kombëtar, luan edhe rolin e CSIRT – it sektorial në rastin e disponimit të infrastrukturave kritike dhe/apo të rëndësishme të informacionit.
8. Promovon dhe miraton standarde për procedurat e trajtimit të incidenteve dhe masat për parandalimin e tyre.
9. Zhvillon dhe përditëson skemën e klasifikimit të incidenteve.
10. Publikon statistika vjetore të incidenteve të raportuara.
11. Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) monitoron përmbushjen e detyrave të CSIRT-eve sektoriale të përcaktuara në këtë udhëzim.
12. Organizon dhe koordinon trajnime kualifikuese, periodike për rritjen e kapaciteteve të ekipeve të CSIRT-eve, në fushën e sigurisë kibernetike.

CSIRT kombëtar, në bashkëpunim edhe me organizmat ndërkombëtarë, organizon të paktën një stërvitje vjetore, që simulon një incident të sigurisë kibernetike, me qëllim testimin dhe përditësimin e aftësive mbrojtëse të sistemeve si dhe trajnimin e punonjësve të CSIRT, për menaxhim sa me profesional të incidenteve kibernetike.

Në përfundim të stërvitjes, përgjegjësi/punonjësi pjesëmarrës i CSIRT përgatit një raport të shkurtër për administratorin e OIKI/OIRI mbi përfitimet e marra nga stërvitja.

3. 3 Aftësitë operacionale të ekipit të CSIRT

Struktura e CSIRT është e lidhur ngushtë me strukturën e organizatës ku bën pjesë CSIRT-i. Gjithashtu struktura varet nga qasja e ekspertëve të kualifikuar që do të jenë full-time pjesë e ekipit apo do të punojnë me baza ad-hoc.

Në mënyrë që një CSIRT të jetë efektiv, ai duhet të jetë proaktiv dhe të përcaktojë të paktën tre role kryesore për të ndihmuar në zgjidhjen e incidentit të sigurisë.

1. Ekipi i reagimit ndaj incidenteve të sigurisë kompjuterike (skuadra operacionale teknike) që posedon njohuritë dhe ekspertizën e nevojshme teknike për të zbutur dëmet e incidentit, kryen riparimet e nevojshme, auditime të rregullta, patch-e dhe trajton incidentet.
2. Një ekspert ligjor, i cili harton politikat e nevojshme, këshillon ekipin menaxhues për veprimet e nevojshme ligjore dhe kryen detyra të sigurimit të cilësisë për të siguruar që pozita ligjore e një organizate të jetë e mbrojtur në rastin e një incidenti të sigurisë.
3. Një ekspert komunikimi, i cili ndihmon organizatën të komunikojë siç duhet për incidentin e sigurisë me publikun dhe kanalet e tjera relevante për të demonstruar besim edhe në momente krize, dhe për të lehtësuar komunikimin e hapur dhe adekuat me qëllim mbrojtjen e reputacionit të organizatës.

Një CSIRT tipik udhëhiqet nga menaxheri i përgjithshëm dhe brenda ekipit evidentohen këto role:

√ Skuadra operacionale teknike:
- Udhëheqësi teknik i ekipit
- Ekspertët teknikë që ofrojnë shërbimet e CSIRT
- Hulumtuesit (*researchers*)

Roli	Detyra	Aftësitë
Menaxheri i CSIRT	• Koordinim i përgjithshëm për përgjigje ndaj incidenteve • Komunikim me vendimmarrësit e organizatës • Siguron personelin e duhur, burimet dhe aftësitë e duhura për përgjigje ndaj incidenteve dhe kërkon outsourcing kur është e nevojshme • Teston dhe përditëson në mënyrë periodike Planin për Përgjigje ndaj Incidneteve (PPI) • Dokumenton vendimet, veprimet, procedurat, inputet dhe outputet që i përkasin PPI • Nëse shërbimet realizohen me outsourcing, ai vlerëson dhe kontrollon punën rast pas rasti	• Aftësi të punojë në situata stresi • Njohuri për sistemet IT dhe proceset e punës së organizatës • Njohuri në menaxhim efektiv të personelit • Aftësi të shkëlqyera komunikimi • Aftësi të shkëlqyera organizative • Aftësi vendimmarrëse

Udhëheqësi teknik	• Përgjegjës për punën teknike të ekipit • Raporton tek menaxheri	• Njohuri të shkëlqyera për kërcënimet kibernetike dhe procedurat e përgjigjes së incidenteve • Njohuri të shkëlqyera për strukturën e brendshme të ekipit • Njohuri të shkëlqyera komunikimi
Anëtarët e tjerë të skuadrës	• Reagon ndaj incidenteve sipas PPI • Shpesh merr përgjegjësi për zbulimin e ndërhyrjeve (Intrusion detection) • Jep rekomandime lidhur me dobësitë dhe kërcënimet e reja • Kontribuon në edukimin dhe rritjen e ndërgjegjësimit brenda organizatës	• Aftësi të shkëlqyera teknike që kanë të bëjnë me administrimin e rrjetit, programim, suport teknik ose intrusion detection • Situata më e mirë do të ishte që CSIRT të kishte të paktën një anëtar të aftë në çdo aspekt të rëndësishëm teknologjik • Të specializuar në fusha teknike si zbulimi i ndërhyrjeve në rrjet, analiza *malware* ose *forensics*. • Aftësi në zgjidhje problemesh dhe të menduarit kritik

Tabela 2 Përgjegjësitë e skuadrës operacionale të CSIRT

√ Ekipi mbështetës:

- Konsulenti ligjor
- Konsulenti i komunikimit

Roli	Detyra	Aftësitë
Konsulenti ligjor	**Përpara ndodhjes së incidentit** • Rishikon PPI për përputhje me legjislacionin në fuqi • Harton format lajmërimi për çdo lloj incidenti • Këshillohet me konsulentin e komunikimit për redaktime në formatin e lajmërimit për media duke i dhënë prioritet ruajtjes së informacionit konfidencial dhe interesave të organizatës	• Të njohë kuadrin ligjor të sigurisë kibernetike • Eksperiencë në hartimin e marrëveshjeve • Eksperiencë në përballje me agjencitë ligj zbatuese • Aftësi për zgjidhje problemesh • I mirë përgatitur dhe i mirë organizuar për të reaguar siç duhet dhe me shpejtësi në çdo situatë.

	• Harton formatet për marrëveshjet e ndarjes së informacionit **Gjatë ndodhjes së incidentit** • Nëse është e nevojshme, plotëson njoftimin për incidentin e ndodhur me konsulentin e komunikimit, dhe sigurohet që njoftimi të bëhet i ditur në kohën e duhur • Kur është e nevojshme ndihmon me mbledhjen e evidencave • Siguron dokumentimin e ngjarjeve siç duhet duke konsideruar hapjen e çështjeve ligjore ndaj organizatës në çdo kohë • Mund të shërbejë si pikë kontakti me agjencitë ligjzbatuese	

Tabela 3 Përgjegjësitë e konsulentit ligjor të CSIRT

Roli	Detyra	Aftësitë
Konsulenti i komunikimit	• Ndihmon në krijimin e politikës së komunikimit për çështjet ligjore dhe menaxheriale • Menaxhon komunikimin me publikun • Menaxhon komunikimin me median • Menaxhon komunikimin me punonjësit e organizatës • Vepron si pikë kontakti për çdo komunikim përveç agjencive ligj zbatuese • Dërgon njoftime për incidente sigurie drejt	• Të njohë politikat e organizatës • Të kuptojë detyrimet ligjore, sidomos ato që lidhen me përpunimin e informacioneve sensitive dhe personale • Të kuptojë punën e CSIRT-it • Aftësi të shkëlqyera komunikimi

	palëve të interesit pas konsultimit me konsulentin ligjor	

Tabela 4 Përgjegjësitë e konsulentit të komunikimit të CSIRT

√ Konsulentët e jashtëm:
- Punësohen sipas nevojave të organizatës

Prania e një konsulenti ligjor është shumë e rëndësishme, sidomos në fazat fillestare të ngritjes së CSIRT. Mund të mendoni se do rrisë kostot, por në fund do t'ju kursejë kohë dhe probleme ligjore.

Në varësi të shumëllojshmërisë së ekspertizës që CSIRT do ofrojë, sidomos në rastet kur organizata ka profil të lartë mediatik, është shumë e rëndësishme prania e një eksperti komunikimi. Këta të fundit, do të realizojnë përkthimin e çështjeve teknike në mesazhe të kuptueshme për median dhe publikun. Eksperti i komunikimit do të shërbejë edhe si urë lidhëse për komunikimin e CSIRT me pjesën tjetër të ekipit, sa herë që do të nevojiten shpjegime për çështje të ndryshme sigurie.

Më poshtë paraqitet skema organizative për strukturën më të shpeshtë të organizimit të CSIRT:

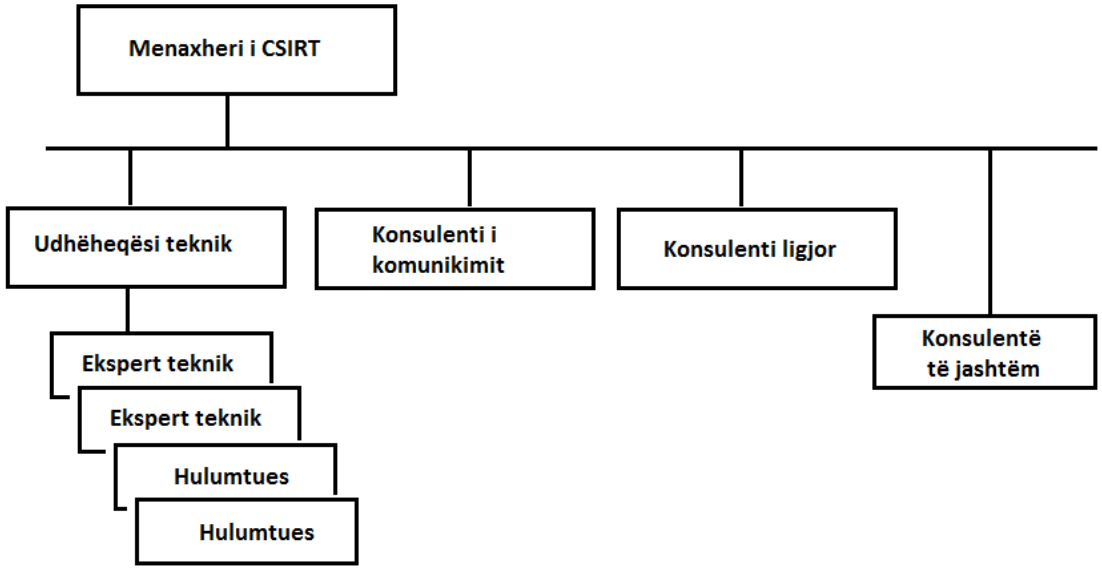


Figura 3 Modeli i pavarur i CSIRT

Në modelin e pavarur të strukturës organizative CSIRT vepron si një organizatë e pavarur dhe e vetme për menaxhimin e punonjësve të ekipit të saj.

3. **4 Shpërndarja e informacionit**

Në këtë kuadër, janë tre elementë që konsiderohen të rëndësishëm:

- besimi dhe ndërtimi i besimit
- cilësia dhe qëndrueshmëria e informacionit dhe reagimi
- skemat dhe terminologjia e përbashkët

Besimi dhe ndërtimi i besimit është një çështje shumë komplekse në të cilët ndikojnë shumë faktorë, prandaj është e vështirë të përcaktohen kërkesa konkrete në këtë fushë. Rekomandohet që të zbatohen udhëzimet e CERT-it Kombëtar në aspektin e bashkëpunimit dhe shpërndarjen e informacionit.

Ndarja e informacionit midis CSIRT-eve mund të jetë e suksesshme vetëm nëse plotësohen dy kërkesa: të gjitha palët e përfshira kontribuojnë në mënyrë të barabartë dhe niveli i cilësisë së informacionit të ofruar është thuajse i barabartë midis gjithë pjesëmarrësve. Kërkesa e parë i detyron CSIRT-et që të marrin pjesë në aktivitetet e shkëmbimit të informacionit për të kontribuar me informacion në mënyrë që të marrin informacion në shkëmbim të informacionit që do japin. Kërkesa e dytë siguron që palët e përfshira në shkëmbimin e informacionit përfitojnë nga informacionet që shpërndan çdo ekip.

Informacioni që shkëmbehet është i kuptueshëm vetëm nëse terminologjia e përdorur nga palët është e kuptueshme njësoj nga të gjithë. Kjo ndihmon në shmangien e paqartësive, dhe si pasojë, në shmangien e reagimeve të gabuara. Ekipet duhet të përdorin skema të ngjashme proceduriale, për shembull për klasifikimin e informacionit ose për enkriptimin e informacionit. Është gjithmonë e këshillueshme që të rishikohet praktika më e mirë dhe të zbatohet aty ku është e mundur dhe e përshtatshme.

4. **Organizimi dhe funksionimi i punës së CSIRT**

4.1 Kriteret e punësimit të stafit

Pas përcaktimit të shërbimeve dhe nivelit të suportit që CSIRT do ofrojë, duhet zgjedhur stafi për realizimin e punës.

Nga pikëpamja e stafit të nevojshëm teknik është thuajse e pamundur të përcaktohet sa ekspertë nevojiten, por ekipi duhet të realizojë detyrat e mëposhtme:

- Në mënyrë që të realizohen shërbimet kyçe të paralajmërimit të incidentit dhe trajtimit të incidentit organizatat ndërkombëtare këshillojnë se nevojiten të paktën 4 ekspertë teknikë full-time
- Për funksionim të plotë të CSIRT-it dhe mirëmbajtje të sistemeve që zotëron organizata, këshillohet të ketë një minimum prej 6 deri 8 ekspertë full-time.
- Për një funksionim 24/7 me dy turne të ekipit, këshillohet që minimumi i ekspertëve teknikë të jetë 12.

Ekspertët teknikë të CSIRT duhet të zotërojnë kompetencat si më poshtë:

Kompetenca personale

- Fleksibël, krijues, aftësi të punojë në skuadër
- Aftësi të forta analitike
- Aftësi për të punuar në situate të vështira
- Konfidencialitet në çështje proceduriale
- Aftësi të mira organizative
- Aftësi shkrimi dhe komunikimi
- Mendje hapur dhe me vullnet për të mësuar

Kompetenca teknike

- Njohuri të gjera mbi teknologjinë dhe protokollet e internetit
- Njohuri në sistemet Linux dhe Unix, në varësi të sistemeve që përdor organizata
- Njohuri në sistemet Windows
- Njohuri mbi pajisjet e infrastrukturës së rrjetit (Router, switch, DNS, Proxy, Mail etj)
- Njohuri mbi aplikacionet e internetit (SMTP, HTTP(s), FTP, SSH etj)
- Njohuri mbi kërcënimet e sigurisë (DDoS, Phishing, Defacing, sniffing etj)
- Njohuri mbi vlerësimin e riskut dhe zbatime praktike

Kompetenca shtesë

- Mundësi të punojë 24/7 ose të jetë i disponueshëm atëherë kur ka emergjenca
- Eksperienca të ngjashme pune në të kaluarën
- Niveli i edukimit sipas profilit të punës

Pozicioni	**Kualifikimet dhe eksperienca**
Menaxheri i CSIRT	• Diplomë bachelor dhe master në shkenca kompjuterike, telekomunikacion dhe të ngjashme me këto.

	• Certifikimet profesionale në fushat CISSP/GCFA/CEH përbëjnë avantazh • Të paktën 5 vjet eksperiencë në fushë
Ekpertët teknikë	• Diplomë bachelor dhe master në shkenca kompjuterike, telekomunikacion dhe të ngjashme me këto. • Certifikimet profesionale në fushat CISSP/GCFA/CEH përbëjnë avantazh • Të paktën 1 vit eksperiencë në fushë
Konsulenti i komunikimit	• Diplomë bachelor dhe master në shkenca kompjuterike, telekomunikacion ose në fushën e komunikimit. • Të paktën një vit eksperiencë në fushë • Njohës shumë i mirë i të paktën një gjuhe europiane, avantazh përbën gjuha angleze
Konsulenti ligjor	• Diplomë bachelor dhe master në shkenca juridike. • Të paktën një vit eksperiencë në fushë • Njohës shumë i mirë i të paktën një gjuhe europiane, avantazh përbën gjuha angleze

4. 2 Siguria fizike dhe përdorimi i pajisjeve

Për shkak se CSIRT kryesisht përpunon informacion sensitiv, rekomandohet që ekipi i CSIRT të aplikojë elementë të sigurisë fizike. Kjo varet nga infrastruktura dhe logjistika e organizatës, si dhe nga politika ekzistuese e sigurisë së informacionit që organizata aplikon.

Funksionimi i një CSIRT-i të ri varet nga bashkëpunimi i organizatës mbi të cilën ngrihet në terma të politikave, rregullave të brendshme dhe çështje të tjera ligjore.

Më poshtë listohen facilitetet kryesore të një CSIRT-i:

Rregulla të përgjithshme të godinës

- Përdorimi i sistemit të kontrollit të aksesit
- Zyra e CSIRT duhet të aksesohet vetëm nga ekipi i CSIRT
- Monitorimi i zyrave dhe hyrjeve me kamera
- Arkivimi i informacionit konfidencial në kasaforta
- Përdorimi i sistemeve të sigurta IT

Rregulla të përgjithshme për pajisjet IT

- Përdorimi i pajisjeve që mund të suportojë organizata
- Mirëmbajtja e sistemeve
- Përditësimi i sistemeve përpara se të lidhen në internet
- Përdorimi i software-ve të sigurisë (Firewall, skanera anti-virus, anti-spyware, etj)

Më shumë informacion përmban aneksi C.

4. 3 Politikat e sigurisë së informacionit

Në varësi të llojit të CSIRT, duhet të hartohet politika e sigurisë së informacionit. Përveç proceseve administrative, proceduriale dhe opeacioniale, politika e sigurisë duhet të jetë në linjë me legjislacionin në fuqi dhe standardet ndërkombëtare të sigurisë. Funksionimi i CSIRT është i kushtëzuar nga ligjet kombëtare dhe rregulloret, të cilat shpesh janë të mbështetura në kontekstin e legjislacionit Europian të fushës, kryesisht mbi direktivat europiane dhe marrëveshjet ndërkombëtare.

Më poshtë listohen ligjet dhe politikat me të cilat duhet të jetë në linjë politika e sigurisë së informacionit për CSIRT-in, të cilat gjenden të linkuara në aneksin E:

Aspekti Kombëtar

- Legjislacioni i fushës mbi teknologjinë e informacionit dhe komunikimit[1]
- Ligjet mbi privatësinë dhe mbrojtjen e të dhënave personale[2]
- Kodet e sjelljes për qeverisjen e internetit[3]

Aspekti europian

- Direktiva mbi Nënshkrimin elektronik (EU/910/2014) [4]
- Direktiva për mbrojtjen e të dhënave dhe privatësinë në komunikimet elektronike GDPR (EU/2016/679)[5]
- Direktiva për rrjetet e komunikimit elektronik dhe shërbimet (2002/19/EC – 2002/22/EC)[6]

Aspekti ndërkombëtar

- Marrëveshja e Basel II (çështjet që lidhen me menaxhimin e riskut operacional)[7]
- Konventa Europiane mbi Krimin Kibernetik (23.11.2001) [8]
- Konventa Europiane e të Drejtave të Njeriut (neni 8 mbi privatësinë)[9]

Standardet

- Standardi BS 7799 (Siguria e Informacionit)[10]
- Standardi ISO 2700X[11]

- IT-Grundschutzbuch, EBIOS dhe të tjera [12]

Për t'u siguruar që CSIRT-i po vepron në përputhje me legjislacionin Kombëtar dhe ndërkombëtar duhet të realizohen konsulta me ekspertin ligjor të ekipit, si dhe të bashkëpunohet me homologët europianë.

Bashkëpunimi me CSIRT-e të tjera europiane

Për të asistuar në zgjidhjen e incidenteve kibernetike nevojitet bashkëpunim me strukturat homologe europiane. Një pikënisje për të bashkëpunim me CSIRT-et europiane është Inventari i aktiviteteve të CERT-eve europiane i publikuar nga ENISA. [3]

Iniciativat Europiane të CSIRT-eve

TF – CSIRT

Task Forca e CSIRT-eve promovon bashkëpunimin midis CSIRT-eve në Europë. Qëllimi kryesor i saj është ofrimi i një forumi për shkëmbimin e njohurive dhe eksperiencave, për të asistuar në mirëfunksionimin e CSIRT-eve të reja.

Kompetencat e Task Forcës janë:

- Ofron forum për shkëmbimin e eksperiencave dhe njohurive
- Krijon shërbime pilote për komunitetin e CSIRT-eve
- Promovon standardet dhe procedurat për përgjigje ndaj incidenteve të sigurisë
- Asiston në krijimin e CSIRT-eve të reja në trajnimin e stafit të tyre

Iniciativat Globale të CSIRT-eve

FIRST[4]

FIRST është lideri global në përgjigjen ndaj incidenteve të sigurisë. Anëtarësimi në FIRST mundëson që ekipet anëtare të përgjigjen më me efektivitet ndaj incidenteve të sigurisë në mënyrë reactive dhe proactive.

[3] Inventari i aktiviteteve nga ENISA http://www.enisa.europa.eu/cert_inventory/
[4] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

FIRST ka anëtarë nga sektorët të ndryshëm duke nisur nga sektori qeveritar, komercial dhe akademik. FIRST ka qëllim të rrisë bashkëpunimin dhe koordinimin midis ekipeve anëtare për të stimuluar reagimin më të shpejtë ndaj incidenteve, dhe promovon shkëmbimin e informacionit midis anëtarëve.

5. Trajtimi i incidenteve

Ky kapitull përshkruan procesin e plotë dhe rrjedhën e punës për trajtimin e incidenteve. Secili hap përshkruhet në paragrafë të shkurtër. Aneksi C jep një panoramë të plotë mbi tools-et e sigurisë.

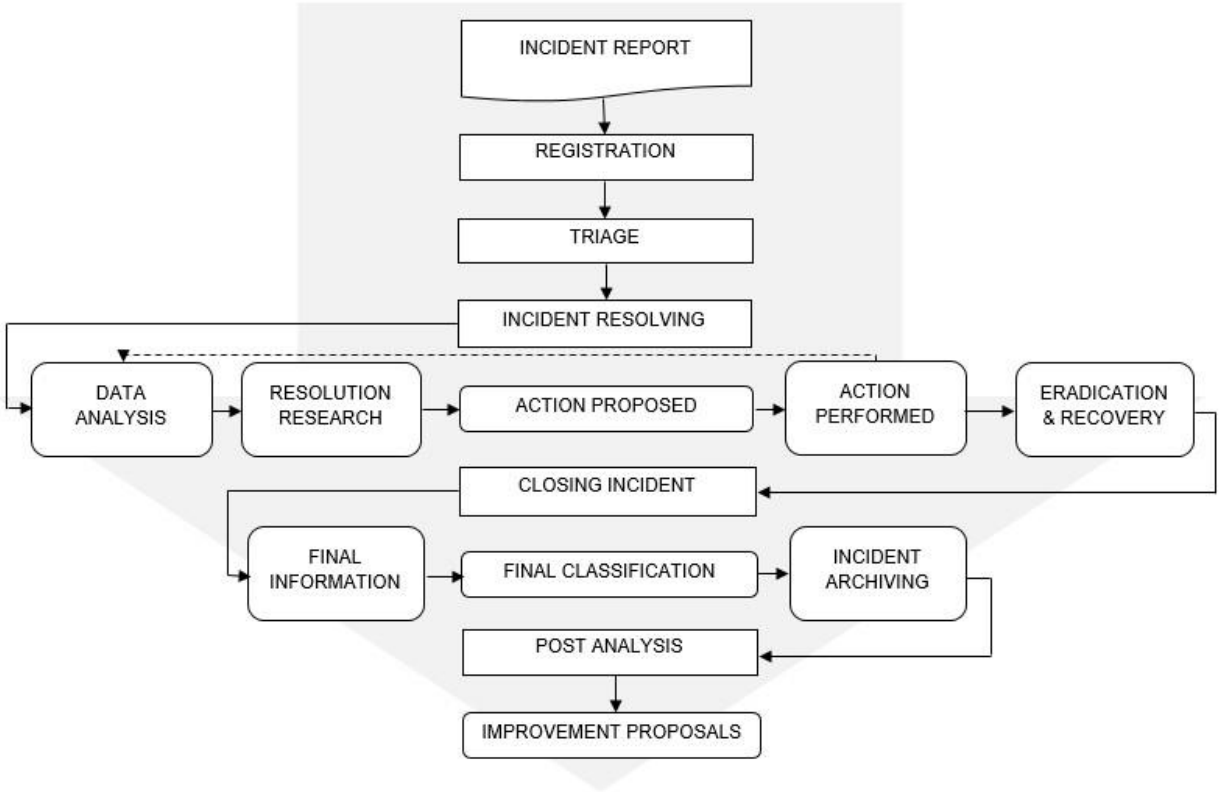


Figure 3: Procesi i trajtimit të incidentit

5.1 Raportimi dhe regjistrimi i incidentit

5.1.1 Raportimi

Raportet e incidenteve gjenden në forma dhe burime të ndryshme.Në aneksin B gjendet një formë raportimi incidentesh kibernetike me të gjithë informacionin e nevojshëm që duhet për të regjistruar dhe trajtuar një incident.

Për të marrë raportimin e një incidenti, skuadra e CSIRT duhet të ketë të publikuar informacionet e mëposhtme:

- E-mail
- Telefon
- Fax
- etj

Në format e komunikimit që vendosni në dispozicion për raportim incidentesh mos harroni të bëheni të pavarur nga interneti. Kjo do të thotë që të vendosni në dispozicion të raportuesve forma kontakti si telefoni, në mënyrë që të jeni të arritshëm për të reaguar edhe nëse interneti është jashtë shërbimit.

Burime të tjera përfshijnë:

- Evente të evidentuara nga rrjeti i brendshëm i monitorimit
- Anëtarësimi i mailing-lista me grupe dhe organizata të
- Anëtarësim në lajmërime automatike në formë të subscription. Për më tepër mund t'i referohen aneksit D mbi burimet e informacionit.
- Radio, televizioni dhe gazetat.

5.1.2 Regjistrimi

Të gjitha raportimet duhet të regjistrohen në bileta (ticket). Bileta do të përdoret gjatë gjithë procesit të trajtimit të incidentit si referencë dhe do të ketë një numër unik identifikues. Numri i referencës së biletës do të përdoret në të gjitha komunikimet mbi të në të ardhmen, komunikime të cilat i referohen specifikisht incidentit të cilin ajo përfaqëson.
Sistemet e regjistrimit të biletave mund të konfigurohen automatikisht duke u lidhur me një adresë emaili. Të gjithë emailet e dërguar drejt asaj adrese do të krijojnë një biletë të re (për incidentet e reja) ose do të shtojnë komunikimin mbi një biletë ekzistuese, në rast se në subjektin e emailit përfshihet numri i referencës së biletës.

Është shumë e rëndësishme që të gjithë incidentet të menaxhohen nga ekipi i CSIRT dhe të trajtohen po nga ky ekip. Kjo është e nevojshme sepse incidente të tjera në të ardhmen do të trajtohen nga e njëjta skuadër dhe zgjidhja do të jepet më shpejt bazuar mbi historikun e trajtimit.
Regjistrimi i centralizuar i incideteve lejon gjithashtu përdorimin e komunikimeve të hershme dhe trajtimeve të ngjashme në të kaluarën.

Sisteme free për përdorimin e biletave të incidenteve janë RTIR (Request Tracker for Incident Response) dhe ORTS (Open Technology Real Services).

5.2 Përzgjedhja

Ky është një nga hapat më të rëndësishëm në procesin e trajtimit të incidenteve sepse merren disa vendime kritike.
Së pari, bëhet verifikimi; a kemi të bëjmë vërtet me një incident? Sa i besueshëm është burimi nga i cili kemi marrë raportimin e incidentit.

Sapo konstatojmë se kemi të bëjmë me një incident kibernetk, CSIRT duhet t'i japë përgjigje pyetjeve të mëposhtme:

- A është incidenti brenda kompetencave të CSIRT-it?
- Cili është ndikimi i incidentit?
- A ka mundësi për dëmtime zinxhir?
- Sa urgjent është zgjidhja e incidentit?
- A mund të rritet dëmi i shkaktuar nga incidenti me kalimin e kohës?
- A ekziston mundësia që incidenti të përhapet?

Përgjigjuni ndaj raportuesit të incidentit

- Bëjuni të ditur që e keni marrë raportimin
- Shpjegojuni se si do të procedohet më tej dhe çfarë duhet të presë raportuesi nga ju
- Sugjerojini çfarë duhet të bëjë ndërkohë, deri në zgjidhjen e incidentit.

Në këtë rast mund të përdoren edhe formularë të gatshëm për përgjigje ndaj incidenteve, sepse ju kursejnë kohë.

5.2.1 Klasifikimi i incidenteve

Klasifikojini incidentet. Mund të mos keni informacion të plotë që në momentin fillestar të raportimit, port ë gjitha këto informacione mund të korrigjohen në një moment të dytë.
Klasifikimi do tju ndihmojë që të përcaktoni prioritetin e trajtimit të incidenteve, si dhe ju ndihmon në përcaktimin e burimeve të nevojshme për trajtimin e mëtejshëm të incidentit.

Më poshtë paraqitet një shembull i përcaktimit të prioritetit të trajtimit të incidenteve nga organizata të mëdha dhe qeveri në botë, sipas burimeve të ENISA-s.

Tabela 5 Prioriteti i trajtimit të incidenteve

Grupi	Prioriteti	Shembull
E kuqe	Shumë i lartë	DDoS, phishing
Portokalli	I lartë	Trojan, akses i paautorizuar
E verdhë	Normal	Spam

Kategorizimi i incidenteve ka funksion shumë të rëndësishë statistikor, sepse e lejon CSIRT të:

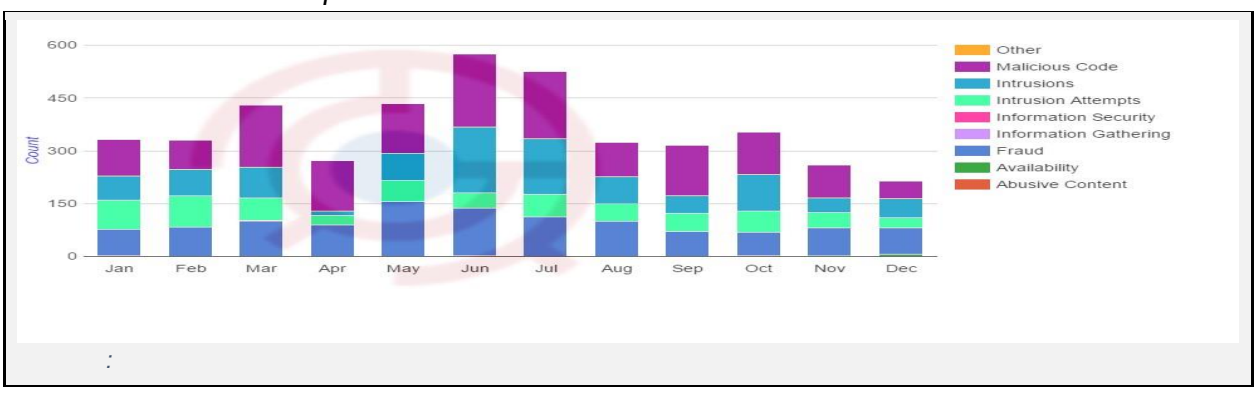
- Njohë trendin e tipeve të incidenteve
- Të ofrojë statistika / grafikë për vendimmarrësit
- Të krahasojë të dhënat që disponon me skuadrat e tjera të CSIRT-eve

Shembuj të klasifikimit të incidenteve mund të gjenden në burimet e mëposhtme:

- Common Language for Incident Response (nga CERT/CC)
- eCSIRT.net taxonomy (zhvilluar gjatë projektit eCSIRT.net)

Gjithashtu klasifikimi i incidenteve mund të realizohet nga vetë anëtarët e ekipit të CSIRT. Kur vendosni të përcaktoni vetë taksonominë e kategorizimit të incidentit, krahasimi me skuadrat e tjera të CSIRT-eve mund të jetë i vështirë. Gjithashtu sigurohuni që të mos krijoni taksonomi shumë komplekse (psh nuk rekomandohet qe të përcaktoni një kategori incidenti për çdo tip malëare); edhe pse kjo mund të krijojë një pamje shumë të detajuar të tipeve të incidenteve që trajton CSIRT-i, do t'ju marrë më shumë kohë përcaktimi i tipit të incidentit sesa zgjidhja e tij.

Një shembull klasifikimi incidentesh bazuar në taksonominë eCSIRT.net gjendet më poshtë.
Tabela 6 Shembull klasifikim incidentesh



Hapi i fundit i kësaj faze është përcaktimi i një ose disa anëtarëve të ekipit për të zgjidhur incidentin, të cilët do të performojnë detyra të tjera në vazhdim deri në zgjidjen e plotë të incidentit ose mbylljen e tij.

5.3 Zgjidhja e incidentit

5.3.1 Analiza e të dhënave

Në këtë hap, duhet të përpiqeni të gjeni sa më shumë informacion të jetë e mundur për të plotësuar panoramën e ndodhjes së incidentit, së bashku me arsyet që çuan në ndodhjen e tij.

Mblidhni të dhëna nga raportimi dhe nga mjedisi i sistemit/sistemeve të prekur nga incidenti:

- Informacione kontakti të detajuara
- Përshkrim i detajuar i incidentit
- Klasifikimi i incidentit siç sugjerohet nga raportuesi i incidentit
- Sistemi i operimit të sistemit dhe të dhëna mbi konfigurimin e rrjetit
- Të dhëna të sakta mbi kohën e ndodhjes së incidentit
- Të dhëna mbi konfigurimin e sistemit të sigurisë së organizatës
- Dëmi që ka shkaktuar incidenti
- Log-e që janë përfshirë në raport

Ka disa vende ku mund të qëndrojnë të dhënat që ju nevojiten:

- Router logs
- Proxy server logs
- Web application logs
- Mail server logs
- DHCP server logs
- Authentication server logs
- Databazat përkatëse të sistemit të prekur
- Firewall ose pajisjet intrusion detection

Në rastet kur informacioni mbi incidentin nuk ndodhet brenda organizatës, duhet të përcaktoni se për çfarë të dhënash keni nevojë, kush i disponon të dhënat që keni nevojë, e pasi të lajmëroni palët që disponojnë këto të dhëna, duhet tu kërkoni akses mbi informacionet që disponojnë.

5.3.2 Zgjidhja

Me të gjitha informacionet e mbledhura në fazën e mëparshme në këtë fazë do të gjendet zgjidhja më e mirë e mundshme e incidentit. Kjo realizohet duke analizuar konkluzione të incidenteve të ngjashme në të kaluarën. Për incidente më komplekse sugjerohet të realizohet brainstorming.

5.3.3 Trajtimi

Në varësi të kompleksitetit të incidentit, një ose disa veprime janë të nevojshme për të trajtuar incidentin.
Përpara se të sugjeroni veprimet që duhen ndërmarrë kini parasysh personat që do ti realizojnë veprimet – ekspertët teknikë do ti kuptojnë zgjidhjet teknike, por nëse nevojitet të ndërmerren veprime që nuk janë teknike por kanë natyrë financiare psh, duhet të përdorni një terminologji të përshtatshme me njerëzit përgjegjës.

Veprimet që mund të sugjerojnë përfshijnë:

- Fikjen e një shërbimi
- Skanimin për malëare
- Realizimi i patching për sistemin
- Izolimi i sistemit ose shërbimit
- Auditimi i sistemit
- Mbledhjen e më shumë informacioneve (ndoshta duke punësuar palë të treta)
- Bkerja e një shërbimi – si psh mbrojtje nga DDoS
- Përshkallëzimi i incidentit drejt ekspertëve ligjorë ose vendimmarrësve të lartë
- Përfshirja e ekspertëve të komunikimit
- Përfshirja e agjencive ligjzbatuese për investigim të mëtejshëm duke e konsideruar krim kibernetike
- Nëse sistemi apo aplikacioni ofrohet nga palë të treta, vendosini në dijeni dhe punoni me ta nëse është e nevojshme

5.3.4 Verifikoni

Verifikoni veprimet që janë ndërmarrë:

- A është targeti i sulmit i arritshëm?
- A u zgjidh incidenti nga trajtimi i realizuar në hapin e mëparshëm?
- A është filtruar siç duhet trafiku?

Nëse targeti i sulmit është ende vulnerabël dhe zgjidhja e propozuar nuk e ka mbyllur incidentin, përsërisni hapat nga 1-3.

5.3.5 Recovery

Pasi incidenti është zgjidhur, sistemi mund të rikthehet në gjendje pune. Kini parasysh që në disa raste rikthimi i sistemit në gjendje pune mund të kërkojë kohë edhe pas zgjidhjes së incidentit, sepse mund të jetë në proces një investigim penal.
Në rast se ekspertët e komunikimit janë përfshirë në incident, sigurohuni që informacionet që do të përcjellin të jenë të përditësuara.

5.4 Mbyllja e incidentit

Duhet të ketë një politikë të qartë se kur nevojitet të mbyllet incidenti, duke qenë se koha e trajtimit të incidentit përbën një statistikë të rëndësishme për organizatën.
Disa skuadra zgjedhin të mos ta mbyllin incidentin, sepse në çdo moment mund të mbërrijë një informacion i ri; disa CSIRT-e vendosin ta mbyllin incidentin kur ai zgjidhet teknikisht, të tjera CSIRT-e mbyllin incidentin vetëm pasi ndërrmerren veprime të tjera si folloë-up i zgjidhjes teknike.

5.4.1 Informacioni final

Sigurohuni që në biletën që përcakton incidentin të jenë të përfshira të gjitha dokumentat shoqëruese. Ky është momenti për të informuar të gjitha palët e përfshira:

- Një përshkrim i shkurtër i asaj që ka ndodhur
- Rezultati i punës
- Gjetjet dhe rekomandimet

5.4.2 Klasifikimi final

Pasi të keni siguruar të gjitha informacinet mbi incidentin duhet të verifikni nëse klasifikimi fillestar ka qenë korrekt. Nëse klasifikimi do tju rezultojë i ndryshëm, konsiderojeni si rekomandim për incidente të tjera të ngjashme në të ardhmen.

5.4.3 Arkivimi i incidentit

Në këtë fazë incidenti mund të mbyllet dhe arkivohet.

Këshillohet që bileta e incidentit të mbyllet por të jetë e disponueshme për qëllime kërkimore për anëtarët e skuadrës CSIRT. Incidente të ngjashme mund të ndodhin në të ardhmen, dhe konsultimi me strategjitë e mëparshme të zgjidhjes së incidenteve do tju kursente shumë kohë.

5.5 Post analysis

Nga një incident mund të mësoni shumë, për ti parandaluar në të ardhmen ose për ti trajtuar më shpejt.

Shembuj të rekomandimeve që mund të zbatoni pas analizës së një incidenti janë:

- Përmirësime të politikës së sigurisë së organizatës
- Përsime në arkitekturën e rrjetit
- Përmirësime në mekanizmat e detektimit

Skuadrat e CSIRT mund ti ndajnë mësimet që kanë mësuar me komunitetin e sigurisë ose homologët e tyre për të përfituar nga njohuritë e fitura.

6. Shërbimet e CSIRT

Sesioni 3.1 përcaktonte listën e plotë të shërbimeve që ofron një CSIRT, siç përcaktohet nga CERT/CC.

Përveç shërbimeve që ofron vetë CSIRT, shërbime të tjera mund të merren në formë outsource. Kjo mund të jetë një zgjidhje e mirë për shërbime të kushtueshme, siç është digital forensics.

6.1 Shërbime reaktive

Shërbimet reaktive shërbejnë për t'iu përgjigjur kërkesave / raporteve të incidenteve nga organizata ku vepron CSIRT dhe çdo kërcënimi apo sulmi ndaj sistemeve të CSIRT. Disa shërbime mund të iniciohen nga njoftime të palëve të treta ose duke analizuar monitorimin ose loget dhe alarmet e IDS.

Alarmet dhe paralajmërimet

Ky shërbim përfshin përthithjen e informacionit që vjen nga një sulm, vulnerabilitet sigurie, alert, virus etj, dhe ofron rekomantime afatshkurtra për tu përballur me problemin. Informacioni mund tu shpërndahet ekspertëve të tjerë të fushës brenda organizatës.

Trajtimi i incidentit

Trajtimi i incidenteve përfshin marrjen, verifikimin dhe reagimin ndaj kërkesave dhe raporteve, si dhe analizimin e incidenteve kibernetike dhe ngjarjeve. Disa prej aktiviteteve në këtë fazë përfshijnë:

- ndërmarrja e veprimeve për të mbrojtur sistemet dhe rrjetet e prekura ose të kërcënuara nga sulmi
- aplikimi i zgjidhjeve dhe strategjive të trajtimit të incidenteve bazuar në rekomandime
- kërkoni për sulme të mundshme në pjesë të tjera të rrjetit
- filtroni trafikun e rrjetit
- realizoni patching të sistemit ose pajisjeve
- zhvilloni strategji të reja për përgjigje ndaj sulmeve

Meqenëse aktivitetet e trajtimit të incidenteve zbatohen në mënyra të ndryshme nga lloje të ndryshme të CSIRT-ve, trajtimi i incidenteve kategorizohet më tej në bazë të llojit të aktiviteteve të kryera dhe llojit të ndihmës të dhënë si më poshtë:

Analiza e incidentit

Ka disa nivele të analizës së incidentit, të cilat shoqërohen me nën-shërbime. Analiza e incidenteve konsiston në ekzaminimin e të gjithë informacionit të disponueshëm dhe evidencat shoqëruese që lidhen me një incident ose ngjarje. Qëllimi i analizës së incidentit është të identifikojë qëllimin e tij, shtrirjen e dëmit, natyrën e incidentit dhe strategjitë e mundshme të përgjigjes.
CSIRT-i mund të përdorë analizën e artifakteve (që përshkruhet më poshtë) për të kuptuar më tepër rreth incidentit dhe sistemit që ka prekur.

CSIRT korrelon veprimtarinë në të gjithë incidentet për të përcaktuar ndonjë ndërlidhje, tendencë ose model. Dy nën-shërbime që mund të bëhen si pjesë e analizës së incidentit, në varësi të misionit, qëllimeve dhe proceseve të CSIRT, janë:

- **Mbledhja e evidencave**

Ky nënshërbim konsiston në mbledhjen, ruajtjen, dokumentimin dhe analizimin e evidencave nga një pajisje e kompromentuar drejt një sistemi. Detyrat që përfshihen në këtë rast janë realizimi i një imazhi të sistemit të prekur, kontrolli për ndryshime si programe të reja, skedarë, shërbime ose përdorues, kontrolli i proceseve që janë duke u ekzekutuar dhe portave të hapura etj.

Stafi i CSIRT që realizon këtë shërbim mund të thirret në procese penale për të dëshmuar mbi evidencat e mbledhura.

- **Gjurmimi**

Gjurmimi i origjinës së sulmit ose identifikimi i sistemit në të cilin sulmuesi ka akses. Ky aktivitet përfshin gjurmimin e mënyrës se si sulmuesi ka fituar aksesin në sistem ose rrjet, cilat sisteme u përdorën për të fituar akses, cila është origjina e sulmit dhe cilat sisteme ose rrjete u përdorën për të realizuar sulmin deri në targetin final. Këtu mund të përfshihet edhe identifikimi i sulmuesit kur është e mundur. Ky shërbim mund të kërkojë bashkëpunim me agjencitë ligjzbatuese, ofruesit e shërbimit të internetit ose palë të tjera të interesit.

Përgjigja e incidentit on site

CSIRT ofron asistencë direkte on-site për të ndihmuar organizatës të rikuperojë pas një incidenti. CSIRT analizon sistemin e prekur dhe realizon riparimin dhe recovery të sistemit fizikisht, në vend që të japë këshilla nëpërmjet e-mailit ose telefonit, siç do të përshkruhet më poshtë. Ky shërbim përfshin të gjithë verimet që duhen ndërmarrë në nivel lokal kur dyshohet se ka ndodhur një incident ose kur incidenti ka ndodhur vërtet. Nëse zyrat e punës së CSIRT nuk ndodhen fizikisht në ambientin ku ka ndodhur incidenti, anëtarët e ekipit teknik duhet të shkojnë ku ka ndodhur sulmi dhe të përgjigjen. Në raste të tjera një skuadër lokale duhet të qëndrojë gjithmonë fizikisht pranë organizatës ku është ngritur dhe të ofrojë shërbime për tu përgjigjur ndaj incidenteve, si pjesë e punës së përditshme.

Suporti i përgjigjes ndaj incidenteve

CSIRT asiston dhe drejton "viktimën" e sulmit për të arritur recovery përmes telefonit, emailit, fax ose dokumentacioneve të tjera shtesë. Kjo mund të përfshijë asistencë teknike në interpretimin e të dhënave të mbledhura, ofrimi i informacioneve të kontaktit ose ndihmë në drejtim të strategjive të minimizimit të dëmit dhe recovery. Në këtë rast nuk ofrohet suport fizikisht, pra on-site si në rastin e shpjeguar më sipëpr. Në këtë situatë CSIRT nuk vepron vetë për të arritur recovery të sistemit apo rrjetit, por vetë personeli që ndodhet pranë sistemit të prekur mund të realizojë recovery.

Koordinimi i përgjigjes së incidenteve

CSIRT koordinon përpjekjet për tu përgjigjur ndaj incidenteve me të gjitha palët e përfshira në incident. Zakonisht këtu përfshihet vetë viktima e sulmit, të tjerë aktorë pranë tij etj. Gjithashtu mund të përfshihen palët që ofrojnë suportin IT për viktimën e sulmit, si ofruesit e shërbimit të internetit, CSIRT-et e tjera partnere, si dhe administratori i sistemit ose rrjetit. Puna koordinuese mund të përfshijë mbledhjen e të dhënave të kontaktit, lajmërimin për hapat që duhen ndërmarrë për palët e përfshira në sulm, mbledhjen e statistikave për numrin e palëve të përfshira, dhe lehtësimin e shkëmbimit të informacionit.
Pjesë e punës koordinuese mund të jetë gjithashtu lajmërimi dhe bashkëpunimi me departamentin ligjor të organizatës, me burimet njerëzore ose me departamentin e marrëdhënieve me publikun. Këto përfshihet edhe bashkëpunimi me agjencitë ligjzbatuese.
Ky shërbim nuk përfshin ndërveprim on-site për përgjigje ndaj incidenteve.

Trajtimi i vulnerabiliteteve

Trajtimi i vulnerabiliteteve përfshin marrjen e informacionit dhe raportimin mbi vulnerabilitete të tipit hardware dhe software; analizimin e natyrës së vulnerabilitetit,

mekanizmat, dhe pasojat e tij; si dhe zhvillimin e stragjive të përgjigjes për të detektuar dhe riparuar sistemin pas sulmit. Meqënëse trajtimi i vulnerabiliteteve realizohet në mënyra të ndryshme nga CSIRT-e të ndryshëm, ky shërbim kategorizohet më tej bazuar në tipin e aktivitetit që realizohet dhe llojit të asistencës që ofrohet, si më poshtë:

Analizat e vulnerabilitetit

CSIRT-i realizon analiza teknike dhe ekzaminime të vulnerabiliteteve në hardware dhe software. Kjo përfshin verifikimin e vulnerabiliteteve të dyshuara dhe ekzaminim teknik të hardware ose software për të përcaktuar se ku ndodhet vulnerabiliteti dhe si mund të luftohet ai. Analiza mund të përfshijë rishikim të kodit burim duke përdorur një debugger për të përcaktuar ku ka ndodhur vulnerabiliteti, ose mund të kopjohet sistemi në një ambjent test për të realizuar gjithë ekzaminimet e nevojshme.

Përgjigja ndaj vulnerabiliteteve

Ky shërbim përfshin përcaktimin e përgjigjes së duhur për të riparuar apo minimizuar dëmin e vulnerabilitetit. Kjo mund të përfshijë zhvillimin e patches etj. Gjithashtu këtu përfshihet lajmërimi për strategjitë e minimizimit të dëmit përmes krijimit të alerteve për palët e interesit.

Koordinimi i përgjigjes së vulnerabilitetit

CSIRT njofton pjesët e ndryshme të organizatës rreth dobësive dhe ndan informacionin për mënyrën e recovery-t ose minimizimit të vulnerabilitetit. CSIRT verifikon nësese strategjia e reagimit ndaj vulnerabilitetit është zbatuar me sukses. Ky shërbim mund të përfshijë komunikimin me shitësit, CSIRT të tjerë, ekspertë teknikë, anëtarë përbërës dhe individë ose grupe që fillimisht zbuluan ose raportuan dobësinë.
Aktivitetet përfshijnë lehtësimin e analizimit të raportit të vulnerabilitetit ose të cënueshmërisë; koordinimin e orareve të prodhimit të dokumenteve korresponduese, patches; dhe sintetizimin e analizave teknike të bëra nga palë të ndryshme. Ky shërbim mund të përfshijë gjithashtu ruajtjen e një arkivi publik ose privat ose regjistrin e njohurive të fituara si pasojë e vulnerabiliteteve të trajtuara dhe strategjive korresponduese të përgjigjeve.

Trajtimi i artifakteve

Artifakti është çdo skedar apo objekt i gjetur në një sistem që mund të përfshihet në hetimin ose sulmin e sistemeve dhe rrjeteve ose që po përdoret për të sfiduar masat e sigurisë së sistemit apo rrjetit.

Artifaktet mund të përfshijnë, por nuk kufizohen vetëm në viruset kompjuterike, programet e Trojanëve, krimbat, skriptet e shfrytëzimit dhe të tjera toolkits-e.
Trajtimi i artifakteve përfshin marrjen e informacionit dhe kopjet e artifakteve që përdoren në sulmet e ndërhyrjeve, zbulimet dhe aktivitetet e tjera të paautorizuara ose shkatërruese.
Sapo të merret, artifakti rishikohet. Kjo përfshin analizimin e natyrës, mekanizmit, versionit dhe përdorimit të artifakteve; dhe zhvillimin (ose sugjerimin) e strategjive të përgjigjes për zbulimin, largimin dhe mbrojtjen nga këto artifakte. Meqenëse aktivitetet e trajtimit të objekteve janë zbatuar në mënyra të ndryshme nga lloje të ndryshme të CSIRT-ve, ky shërbim kategorizohet më tej në bazë të llojit të aktiviteteve të kryera dhe llojit të ndihmës të dhënë si më poshtë:

Analiza e artifaktit

CSIRT kryen ekzaminim teknik dhe analizë të çdo artifakti të gjetur në një sistem. Analiza e bërë mund të përfshijë identifikimin e llojit të skedarit dhe strukturën e objektit, krahasimin e një objektivi të ri kundër objekteve ekzistuese ose versioneve të tjera të të njëjtit artifakt për të parë ngjashmëritë dhe dallimet, reverse engineering ose kodin e disasemblimit për të përcaktuar qëllimin dhe funksionin e objektit.

Përgjigja ndaj artifaktit

Ky shërbim përfshin përcaktimin e veprimeve të përshtatshme për zbulimin dhe heqjen e objekteve nga një sistem, si dhe veprimet për të parandaluar instalimin e objekteve. Kjo mund të përfshijë përditësim të softuerit të antivirusit ose sistemit IDS.

Koordinimi i përgjigjes së artifakteve

Ky shërbim përfshin ndarjen dhe sintetizimin e rezultateve të analizës dhe strategjive të përgjigjeve që i përkasin një artifakti me studiues të tjerë, CSIRT-të, partnerët dhe ekspertët e tjerë të sigurisë. Aktivitetet përfshijnë njoftimin e të tjerëve dhe sintetizimin e analizave teknike nga një shumëllojshmëri burimesh. Aktivitetet mund të përfshijnë gjithashtu ruajtjen e një arkivi publik ose privat të artifakteve të njohura, ndikimin e tyre dhe strategjitë korresponduese të përgjigjeve.

6.2 Shërbimet proaktive

Shërbimet proaktive janë të krijuara për të përmirësuar infrastrukturën dhe proceset e sigurisë të organizatës përpara se ndonjë incident ose ngjarje të ndodhë ose të zbulohet. Qëllimet kryesore janë të shmangen incidentet dhe të zvogëlohet ndikimi dhe fushëveprimi i tyre kur ato ndodhin.

Lajmërimet

Kjo përfshin, por nuk kufizohet vetëm në, alarme për ndërhyrje, paralajmërime të cënueshmërisë dhe këshilla të sigurisë. Njoftime të tilla informojnë anëtarët e organizatës rreth zhvillimeve të reja me ndikim afatmesëm dhe afatgjatë, siç janë dobësitë e reja ose mjetet e ndërhyrjes (intruder tools).
Njoftimet u mundësojnë pjesëmarrësve që të mbrojnë sistemet dhe rrjetet e tyre kundër problemeve të reja të gjetura para se të mund të ndodhin.

Zhvillimet teknologjike

CSIRT monitoron dhe vëzhgon zhvillimet e reja teknologjike, aktivitetet e ndërhyrjeve dhe trendet që lidhen me to për të ndihmuar në identifikimin e kërcënimeve të ardhshme. Temat mund të zgjerohen për të përfshirë studimin e vendimeve ligjore apo legjislative, kërcënime sociale ose politike dhe teknologji të reja. Ky shërbim përfshin leximin e postimeve të sigurisë, faqet e internetit të sigurisë, dhe lajmeve aktuale dhe artikujve të revistave në fushat e shkencës, teknologjisë, dhe politikës për nxjerrjen e informatave relevante për sigurinë e sistemeve dhe rrjeteve përbërëse. Kjo mund të përfshijë komunikimin me palët e tjera që veprojnë në këto fusha për të siguruar që informacioni ose interpretimi është i saktë.
Rezultati i këtij shërbimi mund të jetë një lloj njoftimi, udhëzimi ose rekomandimi i fokusuar në çështjet më të rëndësishme afatmesme dhe afatgjata.

Auditet dhe vlerësimet e sigurisë

Ky shërbim ofron një rishikim dhe analizë të hollësishme të infrastrukturës së sigurisë së një organizate, bazuar në kërkesat e përcaktuara nga organizata ose nga standardet e industrisë që aplikohen. Mund të përfshijë gjithashtu një rishikim të praktikave të sigurisë organizative. Ekzistojnë lloje të ndryshme të auditimeve ose vlerësimeve të sigurisë, duke përfshirë:

- Shqyrtimi i infrastrukturës: Rishikimi manualisht i konfiguracioneve hardware, software, routers, firewalls, serverat dhe pajisjet desktop për të siguruar që ato përputhen me politikat e sigurisë dhe konfigurimet standarde të praktikës më të mirë organizative ose të industrisë.
- Rishikimi i praktikave më të mira: Intervistimi i punonjësve dhe administratorëve të sistemit dhe rrjetit për të përcaktuar nëse praktikat e tyre të sigurisë përputhen me politikën e definuar organizative të sigurisë ose me disa standarde specifike të industrisë
- Skanimi: Përdorimi i skanimit të cenueshmërisë ose viruseve për të përcaktuar se cilat sisteme dhe rrjete janë të cënueshme.
- Penetration testing: Testimi i sigurisë së një organizate duke sulmuar qëllimisht sistemet dhe rrjetet e tij.

Përpara kryerjes së auditimeve ose vlerësimeve të tilla nevojitet të merret miratimi i vendimmarrësve të lartë. Disa nga vlerësimet e mësipërme mund të ndalohen nga politika organizative.
Sigurimi i këtij shërbimi mund të përfshijë zhvillimin e një grupi të përbashkët praktikash kundrejt të cilave kryhen testet ose vlerësimet, së bashku me zhvillimin e një skeme të kërkuar të aftësive ose kërkesat e certifikimit për stafin që kryejnë testimin, vlerësimet, auditimet ose rishikimet. Ky shërbim gjithashtu mund të jepet për një kontraktues si palë e tretë ose për ofrues të shërbimit të sigurisë me ekspertizën e duhur në kryerjen e auditimeve dhe vlerësimeve.

Konfigurimi dhe Mirëmbajtja e Mjeteve të Sigurisë, Aplikacioneve, Infrastrukturës dhe Shërbimeve

Ky shërbim identifikon ose ofron udhëzime të përshtatshme mbi mënyrën e konfigurimit dhe mirëmbajtjes së sigurt të mjeteve, aplikacioneve dhe infrastrukturës së përgjithshme informatike të përdorur nga organizata ose vetë CSIRT. Përveç sigurimit të udhëzimeve, CSIRT mund të kryejë azhornimet e konfigurimit dhe mirëmbajtjen e mjeteve dhe shërbimeve të sigurisë, siç janë IDS, sistemet e skanimit të rrjetit ose të monitorimit, filtrat, firewallet, rrjetet virtuale private (VPN) etj. CSIRT mund t'i ofrojë këto shërbime si pjesë e funksionit të tyre kryesor. CSIRT gjithashtu mund të konfigurojë dhe mirëmbajë serverat, kompjuterët, laptopët, tabletët, smartphonet dhe pajisjet e tjera celulare sipas udhëzimeve të sigurisë. Ky shërbim përfshin përshkallëzimin e menaxhimit të çdo problemi drejt niveleve të larta vendimmarrëse duke e konsideruar sistemin e CSIRT të cënueshëm ndaj sulmeve.

Zhvillimi i tools-eve të sigurisë

Ky shërbim përfshin zhvillimin e çdo mjeti të ri, specifik që kërkohet nga organizata ose nga vetë CSIRT. Kjo mund të përfshijë, për shembull, zhvillimin e patcheve të sigurisë për softuer që përdor organizata ose shpërndarjen e sigurtë të softuerit që mund të përdoret për të rindërtuar hoste të kompromet uar. Mund të përfshijë gjithashtu zhvillimin e mjeteve ose skripteve që zgjerojnë funksionalitetin e mjeteve ekzistuese të sigurisë, si një plug-in i ri për skanuesit e cënueshmërisë së rrjetit, skriptet që lehtësojnë përdorimin e teknologjisë së enkriptimit ose mekanizmat e automatizuar të shpërndarjes së patch-it.

Shërbimet Intrusion Detection

CSIRT-et që kryejnë këtë shërbim shqyrtojnë loget ekzistuese të IDS-it, analizojnë dhe iniciojnë një përgjigje për çdo ngjarje që është brenda kompetencave të tyre ose përcjellin paralajmërimet sipas marrëveshjeve të nivelit të shërbimit të paracaktuara ose strategjive të përshkallëzimit.

Zbulimi i ndërhyrjeve dhe analiza e regjistrave të lidhur me sigurinë mund të mos jetë një detyrë e lehtë - jo vetëm në përcaktimin se ku mund të gjenden sensorët në mjedis, por edhe për mbledhjen dhe analizimin e sasive të mëdha të të dhënave të mbledhura. Në shumë raste, kërkohen mjete ose ekspertiza të specializuara për të sintetizuar dhe interpretuar informacionin për të identifikuar alarmet e rreme, sulmet ose ngjarjet e rrjetit dhe për të zbatuar strategji për eliminimin ose minimizimin e ngjarjeve të tilla. Disa organizata zgjedhin ta transferojnë këtë aktivitet tek të tjerët që kanë më shumë ekspertizë në kryerjen e këtyre shërbimeve, siç janë ofruesit e shërbimeve të menaxhimit të sigurisë.

Shpërndarja e informacionit që lidhet me sigurinë

Ky shërbim i ofron organizatës një koleksion gjithëpërfshirës dhe të lehtë për të gjetur informacion të dobishëm që ndihmon në përmirësimin e sigurisë. Një informacion i tillë mund të përfshijë:

- udhëzimet e raportimit dhe informacionet e kontaktit për CSIRT
- arkivat e alarmeve, paralajmërimeve dhe njoftimeve të tjera
- dokumentacionin rreth praktikave më të mira aktuale
- udhëzime të përgjithshme për sigurinë kibernetike
- politikat, procedurat dhe listat e kontrollit
- informacion mbi zhvillimin dhe shpërndarjen e patch-it
- lidhjet me partnerët
- statistikat aktuale dhe tendencat në raportimin e incidenteve
- informacione të tjera që mund të përmirësojnë praktikat e përgjithshme të sigurisë

Ky informacion mund të zhvillohet dhe të publikohet nga CSIRT ose nga një pjesë tjetër e organizatës (IT, burimet njerëzore ose marrëdhëniet me mediat) dhe mund të përfshijë informacion nga burime të jashtme, si CSIRT të tjerë, partnerë dhe ekspertë të sigurisë.

6.3 Shërbimet e menaxhimit të cilësisë së sigurisë

Shërbimet e kësaje kategori nuk janë unike në trajtimin e incidenteve ose në CSIRT në veçanti. Ato janë shërbime për të përmirësuar sigurinë e përgjithshme të një organizate. Duke shfrytëzuar përvojat e fituara në ofrimin e shërbimeve reaktive dhe proaktive të përshkruara më lart, një CSIRT mund të sjellë perspektiva unike për shërbimet e menaxhimit të cilësisë. Këto shërbime janë të dizajnuara për të inkorporuar reagimet dhe mësimet e nxjerra në bazë të njohurive të fituara duke iu përgjigjur incidenteve, dobësive dhe sulmeve. Përvoja të tilla në shërbimet e përshkruara më poshtë si pjesë e një procesi të menaxhimit të cilësisë së sigurisë mund të përmirësojë përpjekjet afatgjata të sigurisë në një organizatë. Në varësi të strukturave dhe përgjegjësive organizative, një CSIRT mund të ofrojë disa prej këtyre shërbimeve, si më poshtë:

Analiza e riskut

CSIRT-të mund të realizojë analiza dhe vlerësime risku. Kjo mund të përmirësojë aftësinë e organizatës për të vlerësuar kërcënimet reale, për të ofruar vlerësime reale cilësore dhe sasiore të rreziqeve për asetet e informacionit dhe për të vlerësuar strategjitë e mbrojtjes dhe reagimit. CSIRT-të që kryejnë këtë shërbim do të kryejnë ose ndihmojnë në aktivitetet e analizës së riskut të sigurisë së informacionit për sisteme të reja dhe proceset e biznesit ose të vlerësojnë kërcënimet dhe sulmet ndaj aseteve dhe sistemeve përbërëse.

Vazhdimësia e biznesit dhe Planifikimi i Disaster Recovery

Bazuar në ngjarjet e kaluara dhe parashikimet e ardhshme të incidenteve apo trendeve të sigurisë, gjithnjë e më shumë incidentet kanë potencial që të rezultojnë në një degradim serioz të veprimtarive të biznesit. Prandaj, planifikimi duhet të orientohet drejt përvojës së CSIRT dhe në rekomandimet se si t'i përgjigjen incidenteve të tilla për të siguruar vazhdimësinë e operacioneve të biznesit. CSIRT-et që kryejnë këtë shërbim janë të përfshirë në vazhdimësinë e biznesit dhe planifikimin e rikuperimit të fatkeqësive për ngjarjet që lidhen me kërcënimet dhe sulmet e sigurisë kibernetike.

Konsulenca për siguri

CSIRT mund të përdoren për të ofruar këshilla dhe udhëzime për praktikat më të mira të sigurisë për t'u zbatuar për operacionet e biznesit të zgjedhësve. Një CSIRT që ofron këtë shërbim është i përfshirë në përgatitjen e rekomandimeve ose në identifikimin e kërkesave për blerjen, instalimin ose sigurimin e sistemeve të reja, pajisjeve të rrjetit, aplikacioneve softuerike ose proceseve të biznesit të gjerë. Ky shërbim përfshin dhënien e udhëzimeve dhe ndihmës në zhvillimin e politikave të sigurisë organizative.
Mund të përfshijë gjithashtu dhënien këshillave për organet legjiszbatuese ose organeve të tjera qeveritare.

Ndërgjegjësimi

CSIRT duhet të jetë në gjendje të identifikojë se për çfarë kërkojnë më shumë informacion dhe udhëzime anëtarët e organizatës për të qenë në përputhje më të mirë me praktikat e sigurisë dhe politikat e sigurisë organizative. Rritja e ndërgjegjësimit të sigurisë jo vetëm që përmirëson kuptimin për çështjet e sigurisë, por gjithashtu ndihmon në kryerjen e veprimeve të përditshme në një mënyrë më të sigurt. Kjo mund të zvogëlojë ndodhjen e sulmeve dhe të rrisë probabilitetin që zbulimi dhe raportimi të ndodhë më shpejt, duke minimizuar humbjet.

CSIRT-të që kryejnë këtë shërbim rrisin ndërgjegjësimin e sigurisë përmes zhvillimit të artikujve, posterave, gazetave, faqeve të internetit ose burimeve të tjera informative që

shpjegojnë praktikat më të mira të sigurisë dhe ofrojnë këshilla rreth masave paraprake për të marrë.

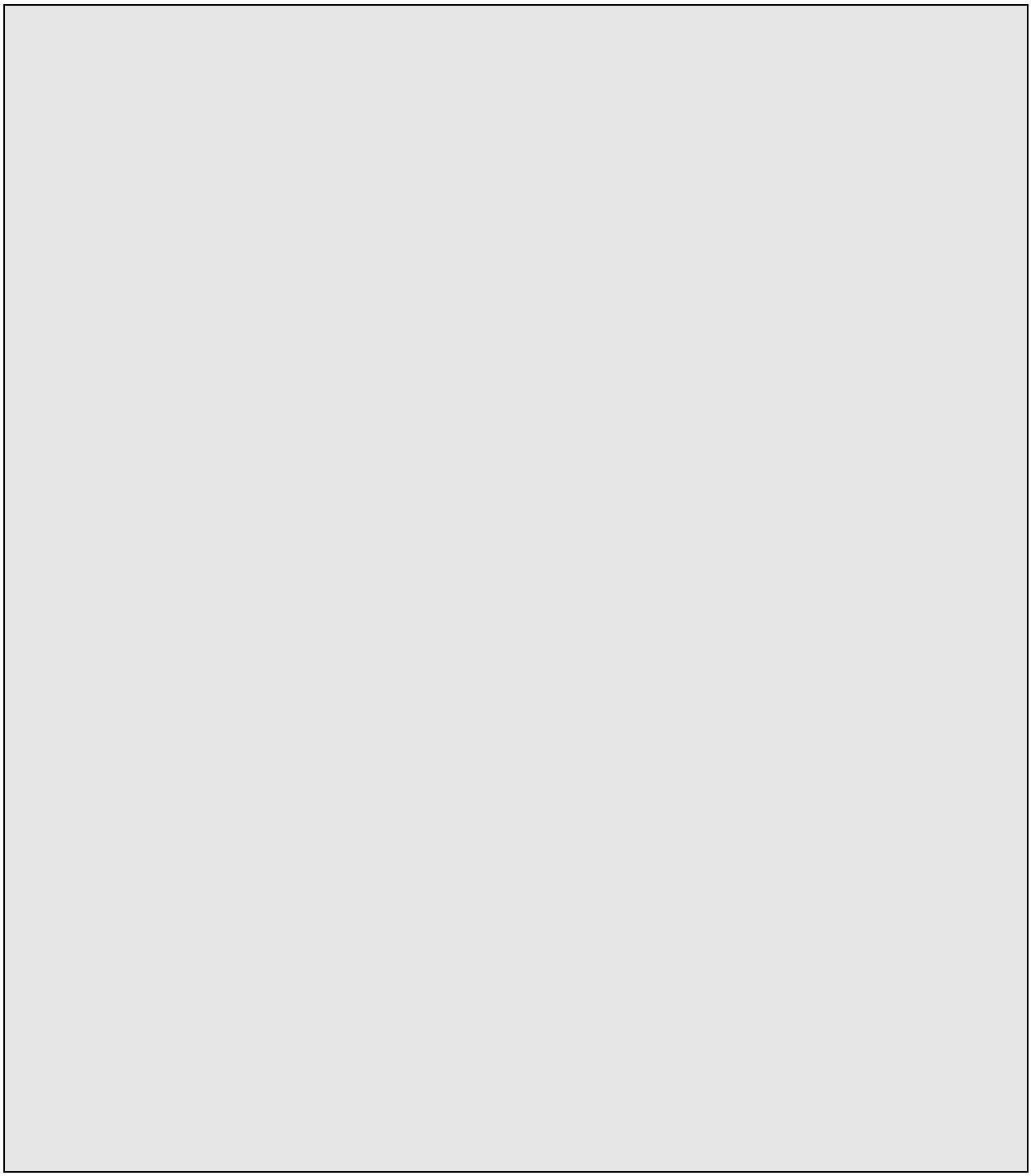
Aktivitetet mund të përfshijnë gjithashtu takime planifikimi dhe seminare për të qenë në kontakt me procedurat e vazhdueshme të sigurisë dhe kërcënimet potenciale ndaj sistemeve organizative.

Edukimi / Trajnimi

Ky shërbim përfshin sigurimin e informacioneve për punonjësit e organizatës rreth çështjeve të sigurisë kibernetike përmes seminareve, workshopeve, kurseve dhe udhëzimeve. Temat mund të përfshijnë udhëzime për raportim të incidenteve, metodat e përshtatshme të reagimit, mjetet e reagimit ndaj incidentit, metodat e parandalimit të incidentit dhe informacione të tjera të nevojshme për të mbrojtur, zbuluar, raportuar dhe për t'iu përgjigjur incidenteve të sigurisë kibernetike.

Aneksi A: Formular i kuadrit të përgjithshëm të CSIRT

Kuadri i përgjithshëm i CSIRT
Emri i CSIRT: Misioni: Institucioni / organizata: Struktura organizative: Disponueshmëria: Shërbimet: Stafi: Infrastruktura and mjetet e disponueshme: Marrëdhëniet me palët e tjera: Modeli i financimit:



Aneksi B: Formular i raportimit të incidentit

FORMULAR RAPORTIMI INCIDENTI

Ju lutem plotësoni formularin dhe përcilleni me email në adresën .....
Fushat me * janë të domosdoshme për tu plotësuar:

Të dhënat e kontaktit:

1. Emri*:
2. Emri i organizatës *:
3. Sektori:
4. Shteti*:
5. Qyteti:
6. E-Mail*:
7. Nr telefoni*:
8. Tjetër:

Hostet e prekura

9. Numri i hosteve:
10. Hostname & IP*:
11. Funsioni i Host-it*:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Software i prekur:
16. Skedrët e prekur:
17. Protocol/port:

Incidenti

18. Numri i referencës ref #:
19. Tipi i Incidentit:
20. Fillimi i incidentit (ora):
21. Ky është një incident i vazhdueshëm: PO JO
22. Ora dhe metoda e zbulimit:
23. Vulnerabilitetet e njohura:
24. Skedarët dyshues:
25. Kundërmasat:
26. Përshkrim i detajuar*:

Aneksi C: Tools-et e sigurisë

Ekzistojnë shumë tools-e për të asistuar CSIRT-et në punën e tyre gjatë trajtimit të incidenteve, dhe shumë prej tyre janë pa pagesë për tu përdorur.

Mos harroni se shumica e skedarëve të logeve ruhen në format "plain text" dhe mund të kërkohen lehtësisht nga command-line si sed, awk dhe grep në Unix/Linux. Të njëjtat mjete mund të përdoren për ti konvertuar në formate të ndryshme me qëllim që të analizohen nga tool-se më të avancuara.

Më poshtë gjeni një listë tools-esh analizimi:

Tabela 7 Tools-et e analizimit

Domain and IP address query tools	
DomainTools	<https://www.domaintools.com/>
Domain Dossier	<http://centralops.net/co/DomainDossier.aspx>
IP to ASN Mapping	<http://www.team-cymru.org/IP-ASN-mapping.html>
GeoLite2	<http://dev.maxmind.com/geoip/geoip2/geolite2/>
RIPEstat	<https://stat.ripe.net/>
E-mail header analysis tools	
Google Apps Messageheader	<https://toolbox.googleapps.com/apps/messageheader/>
MXToolbox	<http://mxtoolbox.com/EmailHeaders.aspx>
Network monitoring tools	
nfdump	<http://nfdump.sourceforge.net/>
nfsen	<http://nfsen.sourceforge.net/>
Network auditing tools	
nmap	<https://nmap.org/>
AutoScan-Network	<http://autoscan-network.com/>
Wireshark	<https://www.wireshark.org/>

AbuseHelper	<https://github.com/abusesa/abusehelper>
Vulnerability assessment tools	
Nessus	<http://www.tenable.com/products/nessus-vulnerability-scanner>
Metasploit	<https://www.metasploit.com/>
Vega	<https://subgraph.com/vega/index.en.html>

OWASP ZAP	<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>
SQLcheck	<http://www.softpedia.com/get/Internet/Servers/Database-Utils/SQLCheck.shtml>
Burp Suite	<https://portswigger.net/burp/>
Kali	<https://www.kali.org/>
Intrusion detection tools	
Snort	<https://www.snort.org/>
Tripwire	<https://sourceforge.net/projects/tripwire/>
Forensic tools	
Sleuth Kit	<http://www.sleuthkit.org/>
Autopsy	<http://www.sleuthkit.org/autopsy/>
Tcpxtract	<http://tcpxtract.sourceforge.net/>
EnCase	<https://www.guidancesoftware.com/encase-forensic>
FTK, Forensic Toolkit	<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
Malware analysis tools	

VirusTotal	<https://www.virustotal.com/>
Malware Domain List	<http://www.malwaredomainlist.com/>
Malware Hash Registry	<http://www.team-cymru.org/MHR.html>
MISP, Malware Information Sharing Platform	<https://mispriv.circl.lu/>
AlienVault Open Threat Exchange	<https://otx.alienvault.com/>
Malwr	<https://malwr.com/>
Hybrid Analysis	<https://www.hybrid-analysis.com/>
Honeypots	
honeyd	<http://www.honeyd.org/index.php>
WiFi tools	
inSSIDer	<http://www.metageek.com/products/inssider/>
Acrylic WiFi Scanner	<https://www.acrylicwifi.com/en/wlan-software/wlan-scanner-acrylic-wififree/>
SIEM tools	
Splunk	<http://www.splunk.com/>
Encryption tools	
GnuPG	<https://www.gnupg.org/>
VeraCrypt	<https://veracrypt.codeplex.com/>

Incident-tracking tools	
RTIR	<https://bestpractical.com/>
OTRS	<https://www.otrs.com/>
Databases	
SQLite	<https://www.sqlite.org/>
MySQL	<https://www.mysql.com/>
PostgreSQL	<https://www.postgresql.org/>

Aneksi D: Burimet e informacionit

Për të marrë lajmërime mbi incidentet, ekzistojnë disa forume që shpërndajnë informacione të besueshme për komunitetin e sigurisë, dhe shumica e këtyre lajmeve janë falas. Më poshtë gjeni një listë burimesh:

Lajmërimet e incidenteve		
APWG, Anti-Phishing Working Group	<http://apwg.org/>	□ Phishing
PhishTank	<http://www.phishtank.com>	□ Phishing
Dark-H	<http://dark-h.org>	□ Web defacements
Mirror-Zone	<http://mirror-zone.org>	□ Web defacements
Zone-H	<http://zone-h.org>	□ Web defacements
Zone-HC	<http://zone-hc.com>	□ Web defacements
Shadowserver	<https://www.shadowserver.org>	□ Botnet □ Open DNS resolver □ Open proxy server □ etc.
Team Cymru	<http://www.teamcymru.org/services.html>	□ Botnet □ Brute force □ DDoS □ Malware URL □ Open DNS resolver □ Open proxy server □ Phishing □ Scanning

Për të gjetur informacione kontakti mbi skuadrat që kanë qenë të përfshira në një sulm, mund të bazoheni në burimet e mëposhtme:

Informacione kontakti për CSIRT-et	
FIRST, Forum of Incident Response and Security Teams	<https://www.first.org/>
APCERT, Asia Pacific CERT	<http://www.apcert.org/>
Trusted Introducer	<https://www.trusted-introducer.org/>
AfricaCERT	<http://www.africacert.org>
Latin American CSIRTs	<http://www.lacnic.net/en/web/lacnic/csirts>
OIC-CERT, Organisation of the Islamic Cooperation CERT	<http://www.oic-cert.org/>
NatCSIRT, National CSIRTs	<http://www.cert.org/incident-management/national-csirts/national-csirts.cfm>

Aneksi E Legjislacioni për hartimin e politikës së sigurisë

[1] http://cesk.gov.al/legjislacioni/index.html

[2] http://www.idp.al/legjislacion/

[3] http://www.plus.al/download/Kodi-i-sjelljes-07-02-2013.pdf

[4] http://cesk.gov.al/wp-content/uploads/2016/04/REGEUR.pdf

[5] https://gdpr-info.eu/

[6] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/corporate-governance/directive-2002-19-ec

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/corporate-governance/directive-2002-22-ec

[7] https://www.princeton.edu/~markus/teaching/Eco467/10Lecture/Basel2_last.pdf

[8] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[9] https://www.echr.coe.int/Documents/Convention_ENG.pdf

[10] https://www.enisa.europa.eu/topics/threat-risk-management/risk- management/current-risk/laws-regulation/rm-ra-standards/bs-7799-3

[11] https://www.iso.org/isoiec-27001-information-security.html

[12] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ebios.html