REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 1085 Prot Tiranë më 18.12.2024

URDHËR

Nr.458 datë. 18.12.2024

PËR

"MIRATIMIN E RREGULLORES MBI PROCEDURAT E MENAXHIMIT TË INCIDENTEVE TË SIGURISË KIBERNETIKE, KUNDËRMASAT, PLAYBOOKS DHE MASAT MBROJTËSE TË NATYRËS SË PËRGJITHSHME"

Në zbatim të shkronjës "k", të nenit 13, pikës 3 dhe 4 të nenit 22 të ligjit nr.25/2024 "Për sigurinë kibernetike",

URDHËROJ

1. Miratimin e rregullores "Mbi procedurat e menaxhimit të incidenteve të sigurisë kibernetike, kundërmasat, playbooks dhe masat mbrojtëse të natyrës së përgjithshme" sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, CSIRT-et sektoriale, si dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI TAFA

REPUBLIKA E SHQIPËRISË - AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE - KËSHILLI I MINISTRAVE

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Rregullore mbi procedurat e menaxhimit të incidenteve të sigurisë kibernetike, kundërmasat, playbooks dhe masat mbrojtëse të natyrës së përgjithshme

PËRMBAJTJA

1. Hyrje 3
1.1 Objekti dhe qëllimi 4
1.2 Subjekte përgjegjëse 4
1.3 Përkufizime 4
2. Cikli i menaxhimit të incidentit kibernetik 5
2.1 Përgatitja në ngritjen e kapaciteteve njerëzore, teknologjike dhe proceseve 7
2.2 Zbulimi i incidentit kibernetik 9
2.3 Identifikimi i incidentit kibernetik 9
2.4 Nisja e procesit të komunikimit dhe koordinimit me Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, Partnerët Ndërkombëtarë, etj 10
2.5 Regjistrimi i incidentit 11
2.6 Kategorizimi 11
2.7 Prioritizimi i Incidentit 11
2.8 Analiza e incidentit 12
2.9 Izolimi, Fshirja dhe Rikthimi i Shërbimit/Dhënave 12
2.10 Suporti për Izolimin, Fshirjen dhe Rikthimin e Shërbimit/Dhënave 13
2.10.1 Reagimi ndaj Incidentit (Izolimi) 13
2.10.2 Pastrimi i sistemeve / rrjeteve të prekura 14
2.10.3 Rikthimi i shërbimit/të dhënave pas incidentit 15
2.10.4 Raporti i incidentit kibernetik 15
2.11 Aktiviteti pas-incidentit 16
ANEKS 1: Skema e menaxhimit të incidentit kibernetik 18
ANEKS 2: Mjetet e rekomanduara për monitorim dhe analizë incidentesh. **Error! Bookmark not defined.**
ANEKS 3: Playbook-ët e Incidenteve Kibernetike 21

LISTA E TABELAVE

Tabela 1: Fazat e ciklit të menaxhimit të incidentit 6

LISTA E FIGURAVE

Figura 1: Cikli i Menaxhimit të Incidentit Kibernetik 6
Figura 2: Skema e menaxhimit të incidentit kibernetik 18

1. Hyrje

Referuar ligjit nr.25/2024 “Për sigurinë kibernetike”, strukturat përgjegjëse “Për menaxhimin e incidenteve të sigurisë kibernetike” janë: CSIRT-it Kombëtar, CSIRT-it Sektorial dhe CSIRT-it pranë operatorit.

CSIRT-it Kombëtar, ushtron kompetencat e mëposhtme në kuadër të menaxhimit të incidentit:

- Monitoron, analizon dhe menaxhon kërcënimet kibernetike, vulnerabilitetet dhe incidentet në nivel kombëtar dhe ofron asistencë teknike për infrastrukturat kritike dhe të rëndësishme të informacionit sipas kërkesës nga operatorët e infrastrukturave të informacionit.
- Trajton incidentet kibernetike në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese kur dyshon për elementë të krimit kibernetik.
- Mbledh dhe analizon të dhënat nëpërmjet hetimit digjital dhe ofron analizë dinamike të riskut dhe të incidentit, si dhe kryen ndërgjegjësimin për situatën aktuale të sigurisë kibernetike.
- Analizon dhe përgatit masa të natyrës së veçantë sipas incidentit kibernetik dhe i komunikon ato te CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.
- Analizon incidentin për të gjetur shkakun e tij si edhe koordinon aktivitetin me operatorët, CSIRT-et sektoriale, institucionet ndërkombëtare dhe qeveritare kur e shikon të arsyeshme.
- I përgjigjet çdo infrastrukture, në zbatim të procedurave të sigurisë, për të mbështetur në mënyrë aktive zgjidhjen e incidenteve;
- Koordinon me Policinë e Shtetit dhe çdo institucion përgjegjës për të ruajtur dhe mundësuar mbledhjen e provave kur dyshon për elemente të krimit kibernetik apo veprave të tjera penale të lidhura me to në infrastrukturat e informacionit.

CSIRT-it Sektorial ushtron kompetencat e mëposhtme në kuadër të menaxhimit të incidentit:

- Siguron rritje të kapaciteteve të stafit nëpërmjet trajnimeve dhe certifikimeve periodike sipas sektorëve që mbulojnë.
- Sipas rastit, siguron ndihmë për operatorët e infrastrukturave të informacionit, si dhe u vë në dispozicion informacionin e nevojshëm që mund të lehtësojë trajtimin efektiv të incidentit.
- Njofton CSIRT-in Kombëtar menjëherë pasi identifikon incidentin, si dhe e njofton këtë të fundit në rast të zgjidhjes së shpejtë të incidentit të ndodhur në infrastrukturat që administrojnë;

CSIRT-it pranë Operatorit ushtron kompetencat e mëposhtme në kuadër të menaxhimit të incidentit:

- Monitoron rrjetet dhe sistemet e informacionit në infrastrukturën e tyre kritike ose të rëndësishme të informacionit mbi incidente të sigurisë kibernetike apo sulme të mundshme kibernetike.
- Identifikon dhe kategorizon incidentin, si dhe vlerëson shtrirjen dhe dëmin e shkaktuar prej tij.
- Trajton incidentin dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese kur dyshon për elemente të krimit kibernetik apo veprave të tjera penale të lidhura me të.
- Parandalon incidente të ngjashme në të ardhmen duke marrë masa parandaluese.
- Përgatit dhe dërgon pranë CSIRT-it Kombëtar raportet e incidenteve sipas formatit dhe afateve të përcaktuara në këtë ligj dhe në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit.
- Mban dhe ruan kronologjinë e të gjitha provave të incidentit në përputhje me dispozitat e ligjit nr.25/2024 "Për sigurinë kibernetike" dhe legjislacionin në fuqi për mbrojtjen e të dhënave personale.
- Raporton pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial çdo incident të sigurisë kibernetike të ndodhur në infrastrukturat e tyre.

1.1 Objekti dhe qëllimi

Objekti i kësaj rregullore është përcaktimi i procedurave dhe hapat që do të ndiqen për parandalimin, identifikimin, regjistrimin, kategorizimin, prioritizimin, analizimin, rikuperimin dhe raportimin ndaj incidenteve kibernetike, me qëllim ndërhyrjen efektive për zgjidhjen dhe minimizimin e ndikimit të tyre në infrastrukturat e informacionit.

1.2 Subjektet përgjegjëse

Kjo rregullore detajon realizimin e hapave të përcaktuar në pikën 1.1 të kësaj rregulloreje duke përcaktuar detyrat dhe përgjegjësitë e CSIRT-it Kombëtar, CSIRT-it Sektorial dhe CSIRT-it pranë operatorit për të menaxhuar incidentet kibernetike.

1.3 Përkufizime

Termat e përcaktuara në këtë rregullore kanë të njëjtin kuptim me termat e përcaktuara në ligjin nr.25/2024 " Për sigurinë kibernetike", si më poshtë vijojnë:

1. **"Incident i sigurisë kibernetike"** është çdo ngjarje që komprometon disponueshmërinë, vërtetësinë, integritetin, konfidencialitetin e të dhënave të ruajtura, të transmetuara apo të përpunuara ose të shërbimeve të ofruara apo të aksesueshme përmes rrjeteve dhe sistemeve të informacionit.

2. **“Trajtimi i incidentit të sigurisë kibernetike”** janë të gjitha procedurat e nevojshme për parandalimin, identifikimin, analizimin, reagimin dhe rikuperimin ndaj një incidenti të sigurisë kibernetike.

3.**“Kërcënim kibernetik”** është një ngjarje ose veprim i mundshëm, që mund të dëmtojë, të ndërpresë ose të ndikojë negativisht në rrjetet e sistemet e informacionit për përdoruesit e tyre dhe persona të tjerë.

4.**“Vulnerabilitet”** është një dobësi, ndjeshmëri ose defekt i produkteve ose shërbimeve TIK, që mund të shfrytëzohet nga një kërcënim kibernetik.

5.**“Playbooks”** është një udhërrëfyes, i cili tregon një procedurë të mirëpërcaktuar që duhet të ndiqet për menaxhimin e çdo kategorie incidenti të sigurisë kibernetike.

2. Cikli i menaxhimit të incidentit kibernetik

1. Menaxhimi i incidentit kibernetik kalon në disa faza, të cilat detajohen në formë skematike në Aneksin 1 të kësaj rregullore. Procesi i trajtimit të incidentit kibernetik, konsiston në:

a) Përgatitjen dhe ngritjen e kapaciteteve njerëzore, teknologjike dhe proceseve;
b) Zbulimin e incidentit kibernetik;
c) Identifikimin e incidentit kibernetik;
d) Nisja e proçesit të komunikimit dhe koordinimit me infrastrukturat, Partnerët Ndërkombëtarë, etj;
e) Regjistrimin e incidentit kibernetik;
f) Kategorizimin e incidentit kibernetik;
g) Prioritizimin e incidentit kibernetik;
h) Analizën e incidentit kibernetik;
i) Izolimin, fshirjen dhe rikthimin e shërbimit/të dhënave;
j) Suportin për izolimin, fshirjen dhe rikthimin e shërbimit/të dhënave;
k) Aktivitetin post-incident kibernetik.

2. Procesi i trajtimit të incidentit kibernetik përfshin CSIRT-in Kombëtar, CSIRT-in Sektorial dhe CSIRT-in pranë operatorit (Operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit).

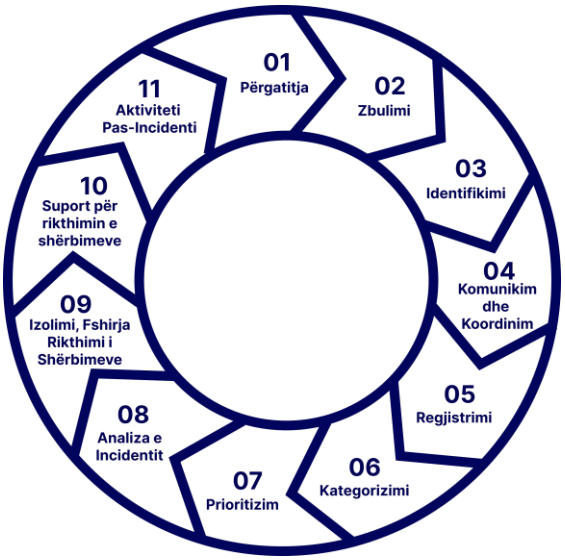

Figura 1: Cikli i Menaxhimit të Incidentit Kibernetik

Tabela 1: Fazat e ciklit të menaxhimit të incidentit

Faza	Përshkrimi
Përgatitja	Përfshin krijimin e politikave të sigurisë, formimin e ekipeve të përgjigjes ndaj incidenteve kibernetike (CSIRT), zhvillimin e strategjive të përgjigjes, përcaktimin e rrjedhave të komunikimit, vendosjen e sistemeve të dokumentimit, sigurimin e mjeteve të nevojshme dhe trajnimin e ekipit për të garantuar gatishmëri në raste incidentesh.
Zbulimi i incidentit kibernetik	Përfshin proceset dhe teknologjitë për monitorimin e rrjeteve dhe sistemeve për të identifikuar aktivitetet e dyshimta, nëpërmjet përdorimit të sistemeve të monitorimit, analizës së trafikut dhe përdorimit të inteligjencës për kërcënime kibernetike me qëllim zbulimin e shkeljeve të mundshme të sigurisë.
Identifikimi i incidentit kibernetik	Përfshin konfirmimin se një aktivitet i dyshimtë përbën një incident kibernetik. Identifikimi i incidentit realizohet nëpërmjet analizimit të alarmeve dhe aktiviteteve të dyshimta për të përcaktuar nëse janë reale dhe të qëndrueshme.
Nisja e proçesit të komunikimit dhe kordinimit me infrastrukturat, Partnerët Ndërkombëtarë, etj.	Përfshin një sërë aktivitetesh kritike që kanë për qëllim të sigurojnë një përgjigje të sinkronizuar dhe të koordinuar ndaj incidentit. Kjo fazë është e rëndësishme për të garantuar se të gjitha palët e interesuara, përfshirë infrastrukturat kritike dhe të rëndësishme të informacionit, partnerët ndërkombëtarë, etj., janë të informuara dhe të angazhuara në mënyrë efektive.

Regjistrimi i incidentit kibernetik	Përfshin dokumentimin e të gjithë informacionit të rëndësishëm rreth incidentit, përfshirë kohën e ndodhjes, natyrën e incidentit, sistemet e prekura dhe veprimet e ndërmarra deri në atë pikë.
Kategorizimi i incidentit	Përfshin kategorizimin e incidentit bazuar në tipin dhe rëndësinë e tij, me qëllim planifikimin e veprimeve për trajtimin dhe zgjidhjen e incidentit të sigurisë kibernetike bazuar në Rregulloren e miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit "Për kategorizimin e incidenteve të sigurisë kibernetike".
Prioritizimi i incidentit kibernetik	Përfshin vlerësimin e rëndësisë dhe ndikimit të incidentit duke marrë parasysh faktorët si ndikimi në infrastrukturë, shkalla e përhapjes dhe rreziku potencial, mbi bazën e të cilit përcaktohet task forca, e cila do të ndërmarrë masat për të reaguar ndaj incidentin si dhe për të analizuar incidentin bazuar në Rregulloren e miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit "Për kategorizimin e incidenteve të sigurisë kibernetike".
Analiza e incidentit kibernetik	Përfshin hetimin e detajuar të incidentit për të kuptuar shkakun, profilin, sjelljen dhe dëmin e shkaktuar. Kjo fazë ndihmon në zhvillimin e strategjive për parandalimin e incidenteve të ngjashme në të ardhmen.
Izolimi, fshirja dhe rikthimi i Shërbimit/ të Dhënave	Përfshin veprimet për të ndaluar përhapjen e incidentit, për të pastruar sistemet e prekura dhe për të rikthyer shërbimet dhe të dhënat në gjendjen e tyre normale. Kjo përfshin përdorimin e mjeteve dhe teknikave për të përjashtuar kërcënimet dhe për të riparuar dëmet e shkaktuara.
Suporti për izolimin, fshirjen dhe rikthimin e Shërbimit/ të Dhënave	Përfshin asistencën që jep CSIRT-it Kombëtar për operatorët e infrastrukturave me qëllin ndalimin e përhapjes së incidentit, për të pastruar sistemet e prekura dhe për të rikthyer shërbimet dhe të dhënat në gjendjen e tyre normale.
Aktiviteti post-incident	Përfshin rishikimin e përgjigjes ndaj incidentit për të identifikuar përmirësimet e mundshme në proceset dhe politikat e sigurisë. nëpërmjet mësimeve të nxjerra, përditësimin e dokumentacionit dhe zhvillimin e strategjive për të parandaluar incidente të ngjashme në të ardhmen, si edhe rifreskimin e programit të trajnimeve.

2.1 Përgatitja në ngritjen e kapaciteteve njerëzore, teknologjike dhe proceseve

Faza e përgatitjes në ngritjen e kapaciteteve njerëzore, teknologjike dhe proceseve përfshin këto hapa:

1. **Krijimin e Politikave të Sigurisë**

Politikat e sigurisë përbëhen nga këto procese:

a) Zhvillimin e politikave gjithëpërfshirëse të sigurisë, bazuar në standardet e mirënjohura ndërkombëtare të sigurisë si ISO 2700x series/NIST 800 xxx series
b) Kryerjen e vlerësimeve të rrezikut dhe pyetësorëve të sigurisë për të identifikuar dhe dokumentuar rreziqet dhe vulnerabilitetet e mundshme të sigurisë.

2. Formimin e Ekipit të Përgjigjes ndaj Incidenteve Kibernetike

Në këtë hap caktohet një ekip për përgjigjen ndaj incidenteve të sigurisë kibernetike CSIRT me role dhe përgjegjësi të përcaktuara.

3. Trajnimin për Përgjigje ndaj Incidenteve

Në këtë hap kryhen trajnime dhe ushtrime të rregullta simuluese për të siguruar gatishmërinë e ekipit, si dhe gjithashtu rishikohet faza e përgatitjes dhe dokumentohen kërcënimet e reja ndërkohë që zbulohen.

4. Zhvillimin e Strategjive të Përgjigjes

Në këtë hap zhvillohenn strategji të përgjigjes që prioritetizojnë rreziqet bazuar në rëndësinë e ndikimit të tyre.

5. Përcaktimin e Rrjedhave të Komunikimit të Incidenteve Kibernetike

Në këtë hap zhvillohet një plan i detajuar komunikimi për të informuar infrastrukturat, palët e interesuara dhe organet e zbatimit të ligjit rreth incidenteve kibernetike. Përcaktohet kontakti për të gjithë anëtarët e ekipit të përgjigjes dhe sigurohet një rrjedhë komunikimi e kriptuar.

6. Mbajtjen e një Regjistri të Incidenteve Kibernetike

Ky hap përfshin mbajtjen e një regjistri për dokumentimin e incidenteve kibernetike, i cili është një komponent thelbësor i përgjigjes ndaj incidenteve. Ky regjistër siguron që të gjitha veprimet dhe detajet e lidhura me incidentet të dokumentohen në mënyrë të strukturuar dhe të qartë. Mbajtja e këtij regjistri ndihmon në menaxhimin dhe zgjidhjen e incidenteve aktuale, por gjithashtu ofron një burim të vlefshëm për analizën dhe përmirësimin e politikave dhe procedurave të sigurisë në të ardhmen.

7. Sigurimin e Mjeteve dhe Burimeve për Përgjigje ndaj Incidenteve kibernetike

Në këtë hap sigurohet disponueshmëria e mjeteve dhe zgjidhjeve të nevojshme për përgjigje ndaj incidenteve. Mjetet e rekomanduara janë të detajuara në Aneksin 2 të kësaj rregulloreje.

8. Kontrollin e Aksesit

Kontrolli i aksesit është një komponent kyç në menaxhimin dhe mbrojtjen e sistemeve dhe të dhënave të një infrastrukture gjatë dhe pas një incidenti kibernetik. Kontrolli i aksesit përfshin implementimin e masave dhe protokolleve të sigurisë me qëllim që të sigurohet vetëm aksesi i personave të autorizuar në burimet e ndjeshme.

2.2 Zbulimi i incidentit kibernetik

Kjo fazë është tranzitore dhe thelbësore për të përcaktuar nëse zbulimi ka të bëjë me një incident apo me të ashtuquajturën "false-positive".

Procesi i zbulimit përfshin, hapat e mëposhtëm:

1. **Monitorimin:** Përdorimi i mjeteve dhe teknologjive për të monitoruar rrjetet dhe sistemet për çdo sjellje të dyshimtë ose jo të zakonshme që mund të tregojë një shkelje të sigurisë.
2. **Alarmet:** Konfigurimi i alarmeve që aktivizohen kur zbulohen aktivitete të dyshimta, duke njoftuar menjëherë ekipet e sigurisë.
3. **Njoftimet:** Informacioni për një incident kibernetik mund të vij nga disa kanale, si:

    a. Platforma e Raportimit të Incidenteve;
    b. E-mail-i;
    c. Shkresë zyrtare nga infrastrukturat,
    d. Rrjetet Sociale si: Kanali Telegram, Facebook, Instagram, etj;
    e. Media të ndryshme;
    f. Nga partnerët kombëtar ose ndërkombëtar,
    g. Telefonit, numri i dedikuar pranë CSIRT-it Kombëtar
4. **Analiza e Trafikut:** Analizimi i trafikut të rrjetit core, perimetrit të rrjetit, të sistemeve fundore përdorues dhe server apo në cloud për të identifikuar modele të papritura ose ndryshime që mund të tregojnë për praninë e një kërcënimi.
5. **Përdorimi i Inteligjencës për Kërcënime:** Shfrytëzimi i të dhënave nga burime të jashtme për të parë nëse ka të dhëna ose informacione të reja rreth kërcënimeve aktuale që mund të ndikojnë në infrastrukturë.

2.3 Identifikimi i incidentit kibernetik

1. Faza e tretë e ciklit të menaxhimit të incidentit kibernetik është identifikimi i incidentit. Identifikimi mund të realizohet nga CSIRT-i Kombëtar, CSIRT-i Sektorial, vetë infrastruktura/ CSIRT-i pranë operatorit, ose nga sisteme të automatizuara që menaxhohen nga struktura përkatëse në **AKSK** dhe edhe pranë operatorëve të infrastukturave.

- Në rastin e identifikimit të incidentit nga CSIRT-ti Kombëtar, apo nga vet operatori i infastrukturës, struktura përkatëse në **AKSK** (SOC T1) dhe CSIRT-i pranë operatorit sipas kategorizimit të incidentit, me qëllim trajtimin e incidentit ekzekuton Playbook-un specifik, referuar Aneksit 3 të kësaj rregulloreje.

2. Identifikimi i Incidentit realizohet nga:

a) Sistemet dhe Punonjësit:

- Punonjësit trajnohen për të njohur dhe raportuar aktivitetet e dyshimta.
- Të gjitha sistemet të kenë mekanizma të përshtatshëm monitorimi dhe alarmi.

b) Identifikimi i Automatizuar: Ngrihen dhe mirëmbahen sistemet e automatizuara (p.sh., SIEM) të menaxhuara nga strukturat përkatëse në AKSK ose/edhe pranë operatorëve të infrastukturave për të monitoruar vazhdimisht dhe për të identifikuar incidente të mundshme.

2.4 Nisja e procesit të komunikimit dhe koordinimit me Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, Partnerët Ndërkombëtarë, etj

Kjo fazë përfshin një sërë aktivitetesh kritike që kanë për qëllim të sigurojnë një përgjigje të sinkronizuar dhe të koordinuar ndaj incidentit. Kjo fazë është e rëndësishme për të garantuar se të gjitha palët e interesuara, përfshirë operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, partnerët ndërkombëtarë dhe organizata të tjera të rëndësishme, janë të informuara dhe të angazhuara në mënyrë efektive. Hapat kryesorë që ndodhin gjatë kësaj faze janë:

1. **Identifikimi i palëve të interesuara**: Në këtë hap, identifikohen të gjitha entitetet që duhet të informohen dhe të përfshihen në përgjigjen ndaj incidentit. Këto mund të përfshijnë operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, partnerët ndërkombëtarë si dhe infrastruktura të tjera qeveritare, të pavarura apo private që mund të kenë një interes ose përgjegjësi në menaxhimin e incidentit.
2. **Vendosja e kanaleve të komunikimit**: Pasi të jenë identifikuar palët e interesuara, hapen kanalet e nevojshme të komunikimit për të siguruar që informacioni të shpërndahet në mënyrë të sigurt. Këto mund të përfshijnë komunikime përmes email-it të sigurt, linja telefonike të dedikuara dhe platforma për ndarje informacioni të klasifikuar.
3. **Koordinimi i përgjigjes**: Në këtë hap, ekipet e ndryshme të përfshira fillojnë të koordinojnë përpjekjet e tyre. Kjo përfshin ndarjen e informacionit të rëndësishëm në lidhje me incidentin, përcaktimin e përgjegjësive specifike për çdo palë, dhe planifikimin e veprimeve të përbashkëta për të adresuar incidentin.
4. **Shkëmbimi i informacionit**: Në këtë fazë, shkëmbehet informacion i përditësuar rreth natyrës së incidentit, ndikimit të tij të mundshëm dhe masave të ndërmarra deri në atë moment. Informacioni duhet të shkëmbehet në mënyrë të sigurt për të shmangur çdo rrezik të kompromet imit të të dhënave.
5. **Monitorimi dhe rishikimi i koordinimit**: Në vijim të komunikimit dhe koordinimit, është thelbësore që të monitorohet vazhdimisht efektiviteti i këtyre proceseve. Duhet të rishikohen dhe të përditësohen planet e përgjigjes sipas nevojës, bazuar në informacionin dhe reagimet e marra nga palët e interesuara.
6. **Dokumentimi dhe raportimi**: Në fund të kësaj faze, të gjitha veprimet e ndërmarra dhe vendimet e marra duhet të dokumentohen në mënyrë të detajuar për të siguruar një gjurmë të qartë të komunikimit dhe koordinimit që është realizuar. Kjo është e nevojshme për analizë pas-incidentit dhe për të nxjerrë mësime për të ardhmen.

Kjo fazë siguron që të gjithë aktorët e rëndësishëm të jenë të angazhuar dhe të informuar për të ndërmarrë masa të sinkronizuara dhe të koordinuara, gjë që është thelbësore për një menaxhim efektiv të incidentit.

2.5 Regjistrimi i incidentit

Faza e pestë e menaxhimit të incidentit kibernetik është regjistrimi i incidentit.

Në rastin e identifikimit të incidentit nga CSIRT-i Kombëtar (SOC T1), regjistrimi i incidentit kryhet nga SOC T1 në minutën e 30 (tridhjetë) pas identifikimit të incidentit. Në rastet e tjera, regjistrimi i incidentit kryhet nga strukturat përkatëse të Mbrojtjes, Menaxhimit dhe Reagimit të Incidenteve Kibernetike pranë AKSK.

Në rastin e identifikimit të incidentit nga CSIRT- pranë operatorit regjistrimi i incidentit kryhet në minutën e 30 (tridhjetë) pas identifikimit të incidentit.

Në secilin rast te identifikimit te incidentit nga CSIRT-i pranë operatorit apo CSIRT-i Kombëtar, regjistrimi i incidentit realizohet në regjistrat sipas formateve të Anekseve III dhe IV të rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike" të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit

2.6 Kategorizimi

Pas regjistrimit të incidentit, kryhet procesi i *triage*, i cili përfshin kategorizimin, prioritizimin, korrelimin dhe caktimin për adresim (*assign for handling)* të incidentit.

Kategorizimi i incidentit bëhet sipas përcaktimeve të nenit 6 të rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike", të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit.

2.7 Prioritizimi i Incidentit

Në këtë fazërealizohet prioritizimi i incidentit kibernetik bazuar në kategorizimin dhe impaktin e këtij incidenti kibernetik. Prioritizimi i incidenteve, bëhet sipas përcaktimeve të nenit 7 të rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike", të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit.

Pas kategorizimit dhe prioritizimit, realizohet korrelimi me incidente të tjera korrente ose me incidentet që kanë ndodhur më parë.

Së fundi, krijohet një *ticket* (planner / *HIVE* / urdhër i brendshëm) për të përcaktuar sektorët përgjegjës që do adresojnë incidentin sipas ciklit të menaxhimit.

2.8 Analiza e incidentit

Analiza e incidentit bëhet nga CSIRT-ti Kombëtar dhe CSIRT-i pranë operatorit dhe konsiston në ekzaminimin e të gjithë informacionit të disponuar dhe evidencat shoqëruese që lidhen me një incident kibernetik të ndodhur. Qëllimi i analizës së incidentit është të identifikojë shkakun e tij, shtrirjen e dëmit, natyrën e incidentit dhe strategjitë e mundshme të përgjigjes.

Task Forca e Analizës dhe Reagimit, e cila ngrihet sipas përcaktimeve te nenit 6 dhe Tabelës 1 të rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike" dhe në përputhje me *ticket* të krijuar në fazën e *triage-t*, mund të përdorë analizën e artifakteve për të kuptuar më tepër rreth incidentit dhe sistemeve të prekura. Analiza e incidentit bazohet në raportin e incidentit të dërguar nga infrastruktura drejt **CSIRT-it Kombëtar**. Task Forca vlerëson nëse është kryer plotësisht izolimi i pajisjeve të prekura dhe jepen rekomandime për izolimin e mëtejshëm.

Analiza e artifakteve konsiston në mbledhjen, ruajtjen, dokumentimin dhe analizimin më të thelluar të kopjeve të logeve, kopje të skedarëve keqdashës, etj.

Procesi i analizës 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 kibernetik, kontrollin nëse ka rrjedhje të të dhënave në Dark web, kontrollin nëse viktima ka degë apo seli në Ballkan/BE/SHBA, etj, dhe nëse po, komunikohet me strukturat përkatëse të Mbrojtjes, Menaxhimit dhe Reagimit të Incidenteve Kibernetike për rrjedhje të të dhënave në këto degë. Këtu mund të përfshihet edhe identifikimi i sulmuesit kur është e mundur.

Procesi i analizës së incidentit mund të kërkojë bashkëpunim me agjencitë ligjzbatuese, autoritetet rregullatore, ofruesit e shërbimit të internetit ose palë të tjera të interesit.

2.9 Izolimi, Fshirja dhe Rikthimi i Shërbimit/Dhënave

Kur incidenti identifikohet nga CSIRT-i pranë operatorit, pas kategorizimit të incidentit sipas përcaktimeve të rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike" si dhe aplikimit të playbook-ut përkatës sipas Aneksit 3 të kësaj Rregulloreje merren masat e menjëherëshme për **izolimin** e pajisjeve fundore dhe sistemeve të prekura shpejt për të parandaluar dëmtime të mëtejshme.

CSIRT-ti pranë operatorit, pas analizës së incidentit kryen vetë ose në bashkëpunim me CSIRT-tin Kombëtar pastrimin e komponentëve të incidentit në sistemet e prekura, si për shembull fshirja e skedarëve keqdashës, çaktivizim i llogarisë së përdoruesit, etj, sipas kategorisë së incidentit. Gjithashtu, kryhen veprimet për të eleminuar kërcënimet kibernetike duke çaktivizuar sistemet e infektuara, duke skanuar për malware dhe duke adresuar vulnerabilitetet.

2.10 Suporti për Izolimin, Fshirjen dhe Rikthimin e Shërbimit/Dhënave

CSIRT-i Sektorial ofron asistencë teknike për infrastrukturat kritike dhe të rëndësishme të informacionit për operatorët e të sektorit përkatës si dhe u vë në dispozicion informacionin e nevojshëm dhe jep zgjidhje konkrete për incidentin.

CSIRT-ti Kombëtar/Task Forca e Analizës dhe Reagimit analizon dhe menaxhon kërcënimet kibernetike, dobësitë dhe incidentin në nivel kombëtar, si dhe ofron asistencë teknike për infrastrukturat kritike dhe të rëndësishme të informacionit sipas kërkesës nga operatorët e infrastrukturave të informacionit.

Gjithashtu, Task Forca trajton incidentet kibernetike në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në legjislacionin në fuqi, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese kur dyshon për elementë të krimit kibernetik.

Të gjitha artifaktet që shoqërojnë analizën e incidentit ruhen në mënyrë të sigurt dhe mbahen për referencë në të ardhmen në rast incidenti të ngjashëm.

2.10.1 Reagimi ndaj Incidentit (Izolimi)

Procedura e reagimit të incidentit është e ndryshme për kategori të ndryshme të incidenteve të raportuara. Hapat e reagimit të incidentit përcaktohen në Playbook-ët e Aneksit 3 të kësaj Rregulloreje.

1. Në momentin që identifikohet incidenti, bazuar në Playbook-ët e Incidenteve Kibernetike jepet suporti për **izolimin** e pajisjeve fundore. Izolohen sistemet e prekura shpejt për të parandaluar dëmtime të mëtejshme. Shembuj përfshijnë shkëputjen e pajisjeve të infektuara, izolimin e segmenteve të rrjetit dhe mbylljen e router-ëve për rrjetet e infektuara.
2. Më pas kryhet një **analizë *forensic*** për të vlerësuar gjendjen e sistemeve të kompromentuara. Për të mbledhur dhe analizuar provat, përdoren mjete të specializuara si *Forensic Tool Kit (FTK).*
3. **Krijohen kopje** rezervë *forensic* të sistemeve të kompromentuara për të mbledhur prova për hetime të ardhshme. CSIRT-ti Kombëtar ruan kopje të logeve të incidenteve të evidentuara apo të raportuara sipas rregullores të miratuar me urdhër të drejtorit të Përgjithshëm të Autoritetit "Për mënyrën dhe afatet e ruajtjes së logeve të incidenteve kibernetike të evidentuara apo raportuara".
4. Implementohen strategji për mbajtje afatgjatë si p.sh. arnimet e sigurisë, heqja e portave, ose riorientimi i trafikut të rrjetit drejt sistemeve të pastra rezervë. Ky hap synon të rifillojë vazhdimësinë e aktivitetit duke rregulluar sistemet e prekura.

Lista Kontrolluese e Fazës së Izolimit

CSIRT-ti Kombëtar/Task Forca e Analizës dhe Reagimit, si dhe CSIRT-i Sektorial në kuadër të izolimit të incidentit orienton CSIRT-in pranë operatorit të zhvillojë check listën e pyetjeve si më poshtë:

- A mund të izolohet incidenti kibernetik?
- A janë izoluar të gjitha sistemet dhe pajisjet e kompromentuara?
- A janë të gjithë pronarët e sistemeve të kompromentuara të vetëdijshëm për incidentin?
- Punoni me pronarët e sistemeve dhe menaxherët e sigurisë për të përcaktuar veprimet e mëtejshme të nevojshme.

Gjatë gjithë kësaj faze të Reagimit ndaj Incidentit identifikohen Treguesit e Kompretimit ***(IOC)*** dhe Treguesit e Sulmit ***(IOA)*** për të përditësuar të gjitha asetet dhe kontrollet e TI/Sigurisë. Rregullat e Fireëall/ËAF/proxy, listat e kontrollit të aksesit ***(ACL)*** dhe bllokimi do të vazhdojnë. Rregulli SIEM *(SIEM Rule),* rasti i përdorimit *(use case),* paneli i kontrollit dhe krijimi, akordimi dhe modifikimi i sinjalizimeve rregullat e zbulimit dhe përgjigjes së pikës fundore ***(EDR),*** nënshkrimet dhe *Blacklist/ Whitelist* do të përditësohen. Hetimi i vazhdueshëm i kërcënimeve përmes analizës së IOC-ve të zbuluara do të vijojë për të përcaktuar hapat e ardhshëm në rehabilitim. Analiza e programeve keqdashëse, klasifikimi dhe çrrënjosja nga sistemet e prekura për të përcaktuar shkakun rrënjësor dhe për të përditësuar asetet dhe shitësit e IT/Sigurisë me inteligjencë mbi IOA dhe IOC, inteligjenca me burim të hapur (OSINT), inteligjenca dhe analiza e kërcënimeve do të bëhen gjithashtu në këtë fazë për të ndihmuar më tej në hetimin dhe riparimin e vulnerabiliteteve.

2.10.2 Pastrimi i sistemeve / rrjeteve të prekura

Pasi incidenti është analizuar, CSIRT-ti Kombëtar/Task Forca me kërkesë të operatorit të infrastrukturës, asiston këtë të fundit në pastrimin e komponentëve të incidentit në sistemet e prekura, si për shembull fshirja e skedarëve keqdashës, çaktivizim i llogarisë së përdoruesit, etj, sipas kategorisë së incidentit. Gjithashtu hiqen kërcënimet kibernetike duke çaktivizuar sistemet e infektuara, duke skanuar për malware dhe duke adresuar dobësitë, me qëllim që të gjitha dobësitë të jenë adresuar dhe dokumentuar.
Pastrimi i sistemeve përfshin:

- Çaktivizimin e sistemeve të infektuara për të forcuar rrjetin kundër sulmeve të vazhdueshme.
- Skanimin e sistemeve të infektuara për gjurmët e malware dhe dobësitë e pa *patch*-uara.
- Adresimin e dobësive në kopjet rezervë të pastra të sistemeve të kompromentuara.

Lista Kontrolluese e Fazës së Fshirjes:

CSIRT-ti Kombëtar/Task Forca e Analizës dhe Reagimit, në fazen e fshirjes së incidentit asiston CSIRT-in prane operatorit të zhvillojë check listën e pyetjeve si më poshtë:

- A mund të forcohen asetet e kompromentuara kundër sulmeve të ngjashme kibernetike?
- A janë pastruar plotësisht asetet e kompromentuara?

- A kanë dokumentuar ekipet e reagimit përpjekjet e tyre të reagimit?
- A janë adresuar të gjitha dobësitë që shkaktuan incidentin kibernetik?

2.10.3 Rikthimi i shërbimit/të dhënave pas incidentit

Pas kryerjes së pastrimit të sistemeve/rrjeteve të prekura, mund të procedohet me rikuperimin e sistemit dhe rikthimin e tij në gjendje pune në rastet kur është e mundur. Të dhënat e rikuperuara duhet të ruhen në një sistem të pastër, i cili duhet të jetë i izoluar nga pjesa tjetër e rrjetit. Gjithashtu, sigurohet që backup që do të përdoret për rikuperimin e të dhënave dhe sistemeve të jetë i pastër.

Në disa raste rikthimi i sistemit në gjendje pune mund të kërkojë kohë edhe pas zgjidhjes së incidentit, sepse mund të ketë nisur një proces hetimi penal. Në rast se ekspertët e komunikimit janë përfshirë në incident, duhet të sigurohen që informacionet që do të përcjellin të jenë të përditësuara.

Sistemet rikthehen në gjendjen e tyre para kompromentimit duke përdorur kopje rezervë të pastra. Gjithashtu bëhet monitorimi për aktivitete të dyshimta dhe zbatohen arnimet e sigurisë për të adresuar dobësitë që shkaktuan ndërhyrjen. Objektivi është të rikthehen sistemet në gjendjen e tyre para kompromentimit. Hapat përfshijnë:

- Zëvendësimin e mjediseve të synuara me kopje rezervë të pastra.
- Monitorimin e sistemeve të rikthyera për aktivitet anormal që tregon infeksione malware.

Lista Kontrolluese e Fazës së Rikuperimit

- A janë zëvendësuar sistemet e kompromentuara me kopje rezervë të pastra?
- A janë adresuar vulnerabilitetet që shkaktuan ndërhyrjen në sistemet e rikthyera?
- A janë monitoruar sistemet e rikthyera për aktivitet të dyshimtë?

2.10.4 Raporti i incidentit kibernetik

Pas rikuperimit të të dhënave, CSIRT-it pranë operatorit përpilon një raport të detajuar sipas përcaktimeve të nenit 23, pika 5 të ligjit 25/2024 “Për sigurinë kibernetike” mbi incidentin, në të cilin evidentohen elementët thelbësor me qëllim për të dokumentuar incidentin, analizuar shkaqet dhe pasojat e tij, si dhe për të identifikuar mësime të rëndësishme që mund të ndihmojnë në parandalimin e incidenteve të ardhmen.

Ky raport jo vetëm që ofron një pasqyrë të qartë të natyrës së incidentit, përfshirë metodat e sulmit, veprat e kryera nga sulmuesit dhe dobësitë e zbuluara në sisteme, por gjithashtu rekomandon veprime specifike për të rritur qëndrueshmërinë kibernetike të infrastrukturës.

Gjithashtu, raporti shërben si një mjet komunikimi me palët e interesuara, duke i informuar ato për rreziqet e identifikuara dhe masat mbrojtëse që janë marrë për t'i zbutur ato, si dhe për të

ndërtuar besim dhe transparencë ndërmjet CSIRT-it Kombëtar dhe infrastrukturave të informacionit.

CSIRT-i pranë operatorit ka detyrimin që të dorëzoj brenda 1 muaji pas njoftimit të incidentit një Raport përfundimtar të incidentit kibernetik pranë CSIRT-it Kombëtar, sipas pikës 5, të nenit 23, të ligjit nr.25/2024 "Për sigurinë kibernetike".

Raporti i incidentit kibernetik është thelbësor jo vetëm për mbylljen e ciklit të menaxhimit të incidentit, por shërben edhe si një instrument kyç për të përmirësuar vazhdimisht strategjitë e sigurisë kibernetike dhe për të forcuar mbrojtjen ndaj kërcënimeve të ardhshme.

Formulari i raportit të incidentit kibernetik duhet të dërgohet me shkresë zyrtare dhe në adresën e postës elektronike: soc@aksk.gov.al.

2.11 Aktiviteti pas-incidentit

1. Mësimet e Nxjerra

Në këtë fazë është e rëndësishme dokumentimi plotësisht i incidentit dhe kryerja e një analizë pas incidentit brenda dy javësh nga momenti i dokumnetimit të tij, identifikimi i fushave që kanë nevoj për përmirësim dhe krijimin e një procesi të optimizuar të reagimit për incidente të ngjashme të ardhshme. Kjo fazë përfshin:

- Rishikimin e të gjithë sekuencës së reagimit ndaj incidentit.
- Thirrjen e ekipeve të reagimit dhe palëve të interesuara për të diskutuar ngjarjen, se si u menaxhua dhe si mund të përmirësohet faza e reagimit.
- Rifreskim të subjekteve të trajnimeve dhe nëse shikohet e arsyeshme nga AKSK, riskedulim i operatorëve.

2. Krijimi i një Strategjie të Reagimit për Incidente të Ardhshme

Menjëherë pas incidenti është mbyllur dhe shërbimet janë rikthyer në gjendje pune infrastruktura duhet të përditësojnë strategjitë e reagimit bazuar në mësimet e nxjerra dhe duhet të kthehen në fazën e përgatitjes, me qëllim dokumentimin e strategjive të reja të reagimit për të përmirësuar reagimet e ardhshme.

3. Raporti i Incidentit

Raporti i incidentit është fazë ku duhet të përqendrohen veprimet pas incidentit, si raportimi i gjetjeve të grupeve të brendshme/të jashtme, personeli dhe palët e interesuara. Në këtë fazë ndiqen të gjitha dorëzimet, gjenerohet një raport teknik që detajon shkakun rrënjësor, krijohet një përmbledhje ekzekutive, veprohet sipas çdo rekomandimi për forcimin e aseteve

IT/Sigurisë si p.sh. (përditësimet e rregullave dhe firmave të Firewall dhe EDR) duke përfshirë përditësimet e dokumentacionit procedural dhe të udhëzimeve.

Lista Kontrolluese e Fazës së Mësimeve të Nxjerra

- A kanë rishikuar të gjithë anëtarët e mbledhjes raportin e plotë të reagimit ndaj incidentit?
- A janë identifikuar fushat për përmirësim?
- A është dokumentuar një proces i optimizuar i reagimit bazuar në fushat e diskutueshme për përmirësim?
- A është përdorur dokumenti i optimizuar i reagimit për të përditësuar/krijuar një strategji reagimi për ngjarje të ngjashme kibernetike në të ardhmen?

Incidentet që nuk kanë nevojë të raportohen janë ato incidente të sigurisë kibernetike sipas përcaktimeve të nenit 11 të Rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike"

ANEKS 1: Skema e menaxhimit të incidentit kibernetik

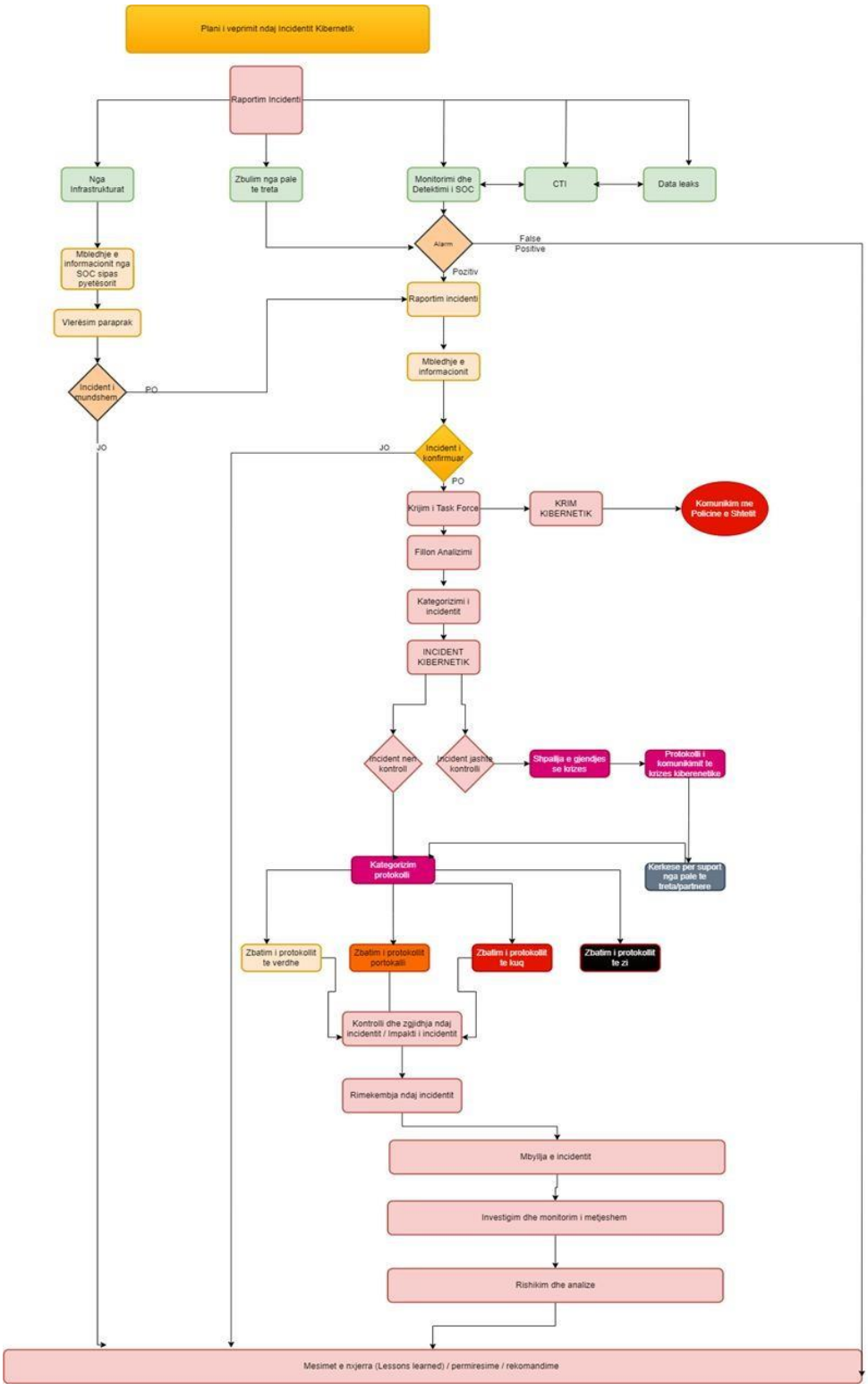

Figura 2: Skema e menaxhimit të incidentit kibernetik

Shënim: Në përputhje me Ligjin 25/2024 "Për Sigurinë Kibernetike", çdo incident i për të cilin dyshohet për element të të krimit kibernetik do të përfshijë menjëherë Policinë e Shtetit. Kjo siguron që të merren të gjitha masat e nevojshme ligjore dhe hetimore menjëherë për të adresuar dhe zbutur ndikimin e incidenteve të tilla.

ANEKS 2: Mjetet e rekomanduara për monitorim dhe analizë incidentesh

Mjetet e rekomanduara për monitorim dhe analizë[1]

Mjetet për analizë të log-eve:

1. **ELK Stack (ElasticSearch + Logstash + Kibana):** Analizë të logeve (SIEM)
2. **Security Onion:** Analizë të logeve (SIEM)
3. **Wireshark:** Analizë të logeve të rrjetit
4. **NetworkMiner:** Analizë të logeve të rrjetit
5. **Chainsaw:** Analizë të logeve Windows
6. **Sysinternals Suite:** Analizë të logeve Windows
7. **Event Log Explorer:** Analizë të logeve Windows
8. **ZUI:** Analizë të logeve Zeek, Network
9. **RITA (Real Intelligence Threat Analytics):** Analizë të logeve Zeek

Disa nga mjetet për Analizë Malware dhe Reverse Engineering:

1. **Ghidra:** Reverse engineering
2. **REMnux:** Malware analysis dhe reverse engineering
3. **Cuckoo.cert:** Malware analysis
4. **x64dbg (X64Debugger):** Malware analysis dhe reverse engineering
5. **Floss:** Malware analysis dhe reverse engineering
6. **CAPA:** Malware analysis dhe reverse engineering
7. **DetectItEasy:** Malware analysis dhe reverse engineering
8. **PE-Bear:** Malware analysis dhe reverse engineering
9. **MD5SUM:** Malware analysis - për gjetjen e HASH të skedarëve
10. **Strings:** Malware analysis - për eksfiltrimin e stringjeve nga skedarët keqdashës
11. **Binwalk:** Malware analysis - për gjetjen e karakteristikave të skedarëve keqdashës
12. **Radare2:** Malware analysis - për gjetjen e karakteristikave dhe instruksioneve të skedarëve keqdashës

[1] Kjo listë nuk është kufizuese për përdorimin e mjeteve të tjera për monitorim dhe analizë

Disa nga mjetet për Shkëmbim dhe Menaxhim të Informacionit të Kërcënimeve të Sigurisë (Threat Intelligence):

1. **MISP Server:** Shkëmbim dhe menaxhim i informacionit të kërcënimeve të sigurisë (Threat Intelligence Platform).
2. **Abuse.ch:** Platformë për ndarjen e informacioneve për malware dhe kërcënime.

Disa nga mjetet për Skanim dhe Zbulim Dobësish/Rrjetesh:

1. **Nikto (Kali Linux):** Skanim i dobësive të aplikacioneve web (Web Vulnerability Scanner).
2. **Nmap:** Skanim i rrjeteve dhe për zbulim hostesh/shërbimesh (Network Scanner).
3. **Spamhaus:** Lista për bllokimin e spam-it dhe zbulim i adresave IP të keqdrejtuara (Spam & Threat Intelligence).

ANEKS 3: Playbook-ët e Incidenteve Kibernetike

Playbook-et e incidenteve kibernetike janë udhëzues standardë operacionalë, të hartuar në përputhje me kuadrin ligjor dhe rregullator, që përcaktojnë hapat për menaxhimin dhe trajtimin e incidenteve kibernetike sipas kategorisë dhe natyrës së tyre. Këto udhëzime mbështeten në standardet kombëtare dhe ndërkombëtare të sigurisë kibernetike, duke siguruar një përgjigje të koordinuar ndërmjet infrastrukturave. CSIRT Kombëtar, garanton përputhshmërinë me legjislacionin përkatës, ofron mbështetje teknike dhe operacionale për CSIRT sektoriale dhe CSIRT pranë operatorëve.

1) Përmbajtja Abuzive

Përmbajtja abuzive i referohet materialeve digjitale të cilat janë të jashtë-ligjshme, të dëmshme ose të papëlqyeshme. Këtu përfshijmë rastet si:

Spam: Është përdorimi i sistemeve elektronike të mesazheve për të dërguar mesazhe të padëshiruara dhe mund dërgohen për qëllime keqdashëse. Forma më e njohur gjerësisht janë e-mail spam.

Shfrytëzimi dhe ngacmimet në internet: ngacmimi i individëve ose bullizimi i tyre përmes internetit.

Fjalor urryes: Material i cili promovon dhunë ose urrejtje ndaj individëve ose grup individësh bazuar në gjininë, besimin, rracën etj.

Abuzimi me fëmijët: Materiale të cilat në fokusin e tyre kanë abuzimin me minorenët.

Përmbajtje terroriste: Materiale të cilat përmbajnë imazhe, video apo tekst i promovuar nga grupe terroristësh.

Keqinformimi apo lajmi i rremë: Informacione të rreme të cilat të udhëheqin drejt keqinformimit.

1.1 Përgatitja

CSIRT Kombëtar

a) Harton politika dhe procedura për identifikimin dhe përgjigjen ndaj përmbajtjes abuzive.
b) Zhvillon dhe mirëmban platformat e inteligjencës së kërcënimit të cilat përfshijnë tregues të përmbajtjes abuzive.
c) Kryen trajnime të rregullta për analistët e CSIRT për zbulimin dhe trajtimin e incidenteve me përmbajtje abuzive.
ç) Siguron pajtueshmërinë ligjore dhe rregullatore në lidhje me monitorimin e përmbajtjes abuzive dhe reagimin ndaj tyre.
d) Përcakton personat që do të menaxhojnë incidentin duke përcaktuar për secilin rolet dhe përgjegjësitë në menaxhimin e incidentit.

CSIRT Sektorial

a) Ofron udhëzime specifike për sektorin për menaxhimin e incidentit rreth përmbajtjes abuzive.

b) Vendos kanale komunikimi brenda sektorit për të raportuar dhe diskutuar përmbajtje të mundshme abuzive.
c) Kryen trajnime të rregullta për personelin e CSIRT sektorial mbi çështjet e përmbajtjes abuzive.
ç) Identifikon asetet dhe platformat kryesore brenda sektorit që mund të jenë objektiv për përmbajtje abuzive(platforma si Media Sociale, Forume ose platforma komunikimi me mesazhe, Cloud Service Provider, Shërbimet e Email-it etj.).
d) Koordinohet me CSIRT-in pranë operatorit me qëllim krijimin e një ekipi monitorimi për zbulimin e hershëm të përmbajtjes abuzive.

CSIRT pranë Operatorit

a) Implementon sisteme për monitorimin dhe filtrimin e përmbajtjes abuzive, me qëllim zbulimin e saj.
b) Trajnon stafin për njohjen dhe raportimin e përmbajtjes abuzive.
c) Zhvillon dhe zbaton politika për përmbajtjen e krijuar nga përdoruesit në platformat e menaxhuara nga operatori.
ç) Krijon një list me kontaktet e besuara për raportimin dhe përshkallëzimin e incidenteve me përmbajtje abuzive.

1.2 Zbulimi

CSIRT Kombëtar

a) Monitoron rrjetin kombëtar dhe platformat sociale për tregues të përmbajtjes abuzive, duke përdorur mjete të zbulimit të anomalive dhe inteligjencës për kërcënimet për të identifikuar shpërndarjen e përmbajtjes keqdashëse
b) Përdor platformat që kanë të integruar Inteligjencën Artificiale dhe *machine-learning* për të automatizuar procesin e zbulimit të përmbajtjes abuzive.
c) Rakordon raportet dhe të dhënat nga burime të ndryshme informacioni dhe identifikon incidentet që lidhen me përmbajtje abuzive.

CSIRT Sektorial

a) Ndan zbulimet dhe gjetjet rreth përmbajtjes abuzive me CSIRT-in kombëtar dhe CSIRT-in pranë operatorit.
b) Monitoron rrjetet sektoriale për anomali të trafikut dhe përmbajtjes, duke përfshirë aktivitetet e papritura të përdoruesve ose përpjekjet e paautorizuara për shpërndarjen e përmbajtjes abuzive.

CSIRT pranë operatorit

a) Përdor mjete për monitorimin e sistemeve dhe rrjeteve për të zbuluar aktivitetet anormale ose përmbajtjen e dyshimtë, si komunikimet e paautorizuara, ndryshimet e papritura në skedarët ose përpjekjet e paautorizuara për të ngarkuar përmbajtje në platformat e brendshme.
b) Konfiguron sisteme automatike që njoftojnë menjëherë në rastet kur identifikohen përpjekje për të shpërndarë përmbajtje abuzive ose kur evidentohen shenja të aktivitetit të paautorizuar në burimet kritike të informacionit.

c) Ruan log-et dhe të dhënat e lidhura me aktivitetin e përmbajtjes abuzive të zbuluar për analizë të mëtejshme dhe përgjigje të specializuar ndaj incidentit.
ç) Skanon sistematikisht përmbajtjen në platformat e brendshme dhe të jashtme për të identifikuar përmbajtjen abuzive që mund të jetë ngarkuar ose shpërndarë pa autorizim.
d) Raporton menjëherë çdo përpjekje të zbuluar për përhapjen e përmbajtjes abuzive drejt CSIRT-it kombëtar dhe atij sektorial, duke ofruar detaje për natyrën dhe burimin e përmbajtjes.

1.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Konfirmon përmbajtjen abuzive përmes analizimit të të dhënave dhe mbledhjes së informacionit nga sisteme inteligjente.
b) Identifikon shtrirjen dhe ndikimin e mundshëm të përmbajtjes abuzive në infrastrukturat kritike dhe të rëndësishme të informacionit.
c) Njofton CSIRT-et sektoriale përkatëse dhe CSIRT-in pranë operatorit për identifikimin e përmbajtjes abuzive.

CSIRT Sektorial

a) Koordinon me CSIRT-in pranë operatorit përmbajtjen abuzive të raportuar nga vetë ai dhe vlerëson ndikimin e incidentit në asestet e sektorit.
b) Jep informacione të detajuara për analizim të mëtejshëm drejt CSIRT-it kombëtar.
c) Koordinohet me CSIRT-in pranë operatorit për të vlerësuar shtrirjen dhe impaktin e incidentit.

CSIRT pranë operatorit

a) Identifikon dhe raporton incidentin për përmbatjen abuzive drejt CSIRT-it kombëtar dhe atij sektorial.
b) Jep informacione të detajuara për analizim të mëtejshëm duke përfshirë burimin e informacionit dhe impaktin.
c) Identifikon nëse përmbajtja është shpërndarë nga brenda ose nga jashtë sistemit të tyre.
ç) Identifikon masat e menjëhershme që duhet të ndërmerren, si bllokimi i përmbajtjes, filtrimi i të dhënave, ose izolimi i përdoruesve të paautorizuar për të parandaluar ndikimin e mëtejshëm të përmbajtjes abuzive.
d) Asiston në procesin e identifikimit duke ndarë log-e dhe të dhëna.

1.4 Komunikimi dhe koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit.
b) Komunikon me autoritetet ligj-zbatuese për një koordinim më efikas në zgjidhjen e problemit.
c) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
ç) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT Sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe palët e interesuara për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informojnë në kohë reale CSIRT kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme

1.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidenteve.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit në mbledhjen e informacionit të nevojshëm dhe për të siguruar që incidenti është dokumentuar plotësisht.

CSIRT Sektorial

a) Koordinohet me CSIRT pranë operatorit të prekur nga incidenti me qëllim regjistrimin e incidentit në platformën e menaxhimit të mundësuar nga CSIRT-i kombëtar dhe siguron që të gjithë operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Mbledh dhe dërgon të dhënat mbi incidentin drejt CSIRT-it kombëtar, duke qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton hapat e ndërmarra në menaxhimin e incidentit rreth përmbajtjes abuzive.
b) Regjistron incidentin në sistemin e menaxhimit të incidenteve sipas procedurës të përcaktuar në rregulloren për kategorizimin e incidenteve të sigurisë kibernetike.
c) Raporton incidentin tek CSIRT-i kombëtar dhe ai sektorial.

1.6 Kategorizimi i incidentit

CSIRT Kombëtar

a) Kategorizon incidentin si "përmbajtje abuzive" bazuar në përmbajtjen e saj pasi konfirmohet si i tillë.
b) Klasifikon incidentin sipas ndikimit në sigurinë kombëtare, sigurinë sigurinë publike dhe stabilitetin social.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit mbi kategorizimin dhe hapat e tjerë që duhen marrë.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit si abuziv si dhe e komunikon atë brenda sektorit.
b) Ndihmon në përcaktimin e natyrës specifike të përmbajtjes abuzive (p.sh., gjuhë urrejtjeje, dezinformim, përmbajtje ilegale).

CSIRT pranë operatorit

a) Kategorizon incidentin me përmbajtje abuzive dhe e raporton atë drejt CSIRT-it kombëtar dhe atij sektorial.
b) Jep informacion rreth natyrës, dhe ndikimit potencial të përmbajtjes.
c) Merr masa të menjëherëshme për zbutjen e ndikimit dhe mos përhapjen e mëtejshëme të incidentit.

1.7 Prioritizimi i incidentit

CSIRT Kombëtar

a) Vlerëson kritikalitetin e përmbajtjes abuzive bazuar në ndikimin që kjo përmbajtje ka në publik dhe në sigurinë kombëtare.
b) Prioritizon incidentin bazuar në përhapjen e përmbajtjes, audiencën, dhe në kritikalitetin e shërbimeve të prekura.
c) Koordinon menaxhimin e incidentit bazuar në përmbajten me ndikimin më të lartë.

CSIRT Sektorial

a) Bashkëpunon me CSIRT-in pranë operatorit në lidhje me vlerësimin e ndikimit të incidentit në shërbimet kritike të sektorit.
b) Koordinohet me CSIRT-in pranë operatorit me qëllim prioritizimin e incidentit duke u fokusuar në fushat me ndikim të lartë me qëllim sigurimin e një reagimi të koordinuar ndaj incidentit.

CSIRT pranë operatorit

a) Vlerëson ndikimin e përmbajtjes abuzive në besimin e publikut.
b) Prioritizon masat mbi reagimin ndaj incidentit duke u fokusuar te kritikaliteti që ky incident ka.
c) Raporton vendimet për prioritizimin drejt CSIRT-it kombëtar dhe atij sektorial bazuar në analizime dhe arsyetime të sakta.

1.8 Analiza e incidentit

CSIRT Kombëtar

a) Kryen analizë të detajuar për të kuptuar origjinën, qëllimin apo ndikimin potencial që përmbajtja abuzive ka.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë si burimin dhe qëllimin e përmbajtjes abuzive.
c) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe CSIRT-in pranë operatorit për të ndihmuar në reagimin ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në identifikimin e dobësive të shfrytëzuara nga sulmuesit për të përhapur përmbajtjen abuzive dhe sugjeron strategji të zbutjes për të parandaluar raste të ngjashme në të ardhmen.
b) Asiston CSIRT-in pranë operatorit në analizimin e mënyrës së përhapjes së përmbajtjes abuzive dhe qëllimin e saj për të përcaktuar nëse përmbajtja është shpërndarë me qëllim që të dëmtojë reputacionin, të përhap panik, apo të përhapë informacione të rreme.
c) Vendos në dispozicion të CSIRT-it kombëtar të dhënat e analizës së operatorëve me qëllim për të shpjeguar situatën dhe shtrirjen e incidentit.

CSIRT pranë operatorit

a) Analizon incidentin në nivel operacional për të kuptuar si është shpërndarë përmbajtja abuzive dhe cili është ndikmi i saj.
b) Analizon rrugët e përhapjes së përmbajtjes abuzive, duke identifikuar përdoruesit, IP-të, aplikacionet ose shërbimet që mund të jenë përdorur për këtë qëllim.
c) Analizon burimin dhe përmbajtjen abuzuese për të identifikuar teknikat e mundshme të aktorëve keqdashës për të përmirësuar mbrojtjen e sistemeve në të ardhmen.
ç) Bashkëpunon me CSIRT-in kombëtar dhe atë sektorial duke ndarë me to të dhëna dhe analizime.
d) Përdor gjetjet për të ndihmuar në reagimin ndaj incidenteve në të ardhmen.

1.9 Izolimi dhe fshirja

CSIRT kombëtar

a) Jep suport për operatorët e infrastrukturave me qëllim izolimin dhe fshirjen e kompotenteve të përmbajtjes abuzive të identifikuar.
b) Ofron udhëzime për izolimin e përmbajtjes abuzive të identifikuar, duke përfshirë metodat për të bllokuar përhapjen e saj nëpër rrjetet kombëtare.
c) Bashkëpunon me institucionet kompetente me qëllim fshirjen e përmbajtjes abuzive nga sistemet dhe platformat kombëtare, duke siguruar heqjen e plotë të saj.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit me qëllim implementimin e masave mbrojtëse për të izoluar sistemet e prekura nga përmbajtja abuzive, duke përfshirë bashkëpunimin me institucionin përgjegjës për bllokimin e IP-ve të burimit, filtrimin e trafikut dhe ndalimin e aksesit në përmbajtjen abuzive në rrjetet sektoriale.
b) Koordinohet me CSIRT-in pranë operatorit për fshirjen e përmbajtjes abuzive.
c) Monitoron situatën për të parandaluar rishfaqjen e përmbajtjes pasi ajo është fshirë.

CSIRT pranë operatorit

a) Izolon menjëherë çdo sistem të prekur nga përmbajtja abuzive, duke ndërprerë aksesin e përdoruesve të paautorizuar dhe duke bllokuar trafikun që përmban përmbajtjen abuzive.
b) Ndjek udhëzimet e CSIRT-it kombëtar dhe atij sektorial për izolimin dhe fshirjen e përmbajtjes abuzive, duke siguruar që të gjitha hapat e nevojshëm të ndërmerren për të parandaluar përhapjen e mëtejshme.
c) Për zbatimin e masave specifike të izolimit dhe fshirjes, CSIRT-i pranë operatorit kryen veprimet e mëposhtme:
   i. Bllokon IP- keqdashëse: Përditëson *firewall* dhe sistemet *IDS/IPS* për të bllokuar çdo IP që ka qenë burim i përmbajtjes abuzive.
   ii. Fshin përmbajtjen në platformat e brendshme: Identifikon dhe fshin të gjitha instancat me përmbajtje abuzive.
   iii. Ndalon aksesin e përdoruesve të kompromentuar: Çaktivizon llogaritë e përdoruesit/ve që kanë qenë të përfshira në shpërndarjen e përmbajtjes abuzive, duke ndryshuar kredencialet dhe duke ndjekur rregullat dhe politikat e aksesit.
   iv. Përdor mjete të automatizuara për të skanuar dhe hequr përmbajtjen abuzive që mund të jetë përhapur në sistemet e brendshme ose të jashtme.
ç) Verifikon që përmbajtja është fshirë dhe e raporton statusin drejt ekipeve përkatëse të CSIRT-it kombëtar dhe atij sektorial.

1.10 Rikthimi shërbimeve/të dhënave

CSIRT Kombëtar

a) Ofron asistencë në rikthimin në gjendje normale të shërbimeve operacionale, platformës dhe shërbimeve.
b) Koordinohet me CSIRT-in pranë operatorit dhe atë sektorial që të gjitha shërbimet e prekura të rikthehen në gjendje punë.
c) Monitoron sistemet pas rikthimit të tyre dhe shmang incidentet në të ardhmen.

CSIRT Sektorial

a) Ofron suport për operatorët e infrastrukturave në fazën e rikthimit të shërbimeve sipas sektorëve përkatës duke prioritizuar shërbimet bazuar në ato që janë prekur më tepër.
b) Suporton operatorët në rikthimin normal të operacioneve si dhe rikthimin e besimit te publikut.
c) Komunikon statusin e rikthimit drejt CSIRT-it kombëtar dhe palëve të treta.

CSIRT pranë operatorit

a) Rikthen shërbimet bazuar nga ato me ndikimin më të lartë.
b) Vërteton integritetin dhe funksionalitetin e shërbimeve të rikthyera.
c) Raporton progresin e rikthimit të shërbimeve dhe çdo problematikë drejt CSRT-it kombëtar dhe atij sektorial.

1.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport me detaje rreth përmbajtjes abuzive, hapat e ndërmarrë për menaxhimin e incidentit dhe përfundimet.
b) Kryen rishikim pas incidentit për të nxjerrë mësime dhe ku ka më tepër nevojë për përmirësim.
c) Ndan raportet me CSIRT-in sektorial dhe CSIRT-in pranë operatorit të infrastrakturës kritike dhe të rëndësishme të informacionit për të përmirësuar reagimin ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Harton për sektorin specifik një raport mbi ndikimin e incidentit dhe hapat e ndërmarrë për menaxhimin e incidentit dhe përfundimet.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke kontribuar në njohuri specifike për sektorin.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar zbulimin dhe aftësitë e përgjigjes në të ardhmen.

CSIRT pranë operatorit

a) Harton një raport përfundimtar në lidhje me ndikimin e incidentit, masat e marra si dhe rikthimin e shërbimeve.
b) Merr pjesë në procesin e mësimeve të nxjerra dhe mban shënim faktorët që ndihmojnë në përgjigjen më të shpejtë të incidentit në të ardhmen.
c) Zbaton rekomandimet për të përmirësuar mbrojtjen ndaj incidenteve mbi përmbajtjet abuzive në të ardhmen.

2) Kod Keqdashës

Me kod keqdashës, ose "*Malicious Code* / *Malware*" do të nënkuptojmë çdo program apo skript të programuar me qëllim për të ndikuar negativisht në një kompjuter, server ose rrjet kompjuterik. *Malware* futet në mënyra të ndryshme në kompjuterin e viktimës. Ai mund të jetë në formën e një kodi ekzekutues, skript, program etj.

Malware mund të përfshijë: viruse kompjuterike, worms, trojan, programe vëzhguese (spyware), rootkits, botnet, regjistrues të tastierës(keyloger), programe për kërkesa shpërblimi (ransomware), programe për gjenerimin e kriptovalutave, kod të dëmshëm për pajisje mobile etj.

Si mund të dallojmë karakteristikat e tyre?

Tabela 2: Karakteristikat e Kodeve Keqdashës

	Natyra	**Dëmi**
Virus	Një program që përsërit vetveten dhe kodi i të cilit injektohet në mënyrë shumë komplekse në programet legjitime.	Përhapja, korruptimi si dhe shkatërrimi i të dhënave.
Worm	Një program që përhapet vetvetiu përmes rrjetit ose mediave të tjera të transferimit.	Shpejtësi e lartë e përhapjes dhe mundësia e shkatërrimit masiv.
Trojan	Një program i fshehur brenda një programi ose aplikacioni të zakonshëm duke shkaktuar dëme kur ekzekutohet.	Shkatërrimi i të dhënave, shpërndarja e informacionit të fshehur.
Spyware	Një program që fshehurazi mbledh informacione rreth aktivitetit të një përdoruesi pa dijeninë e tyre.	Kufizimi i privatësisë, vjedhja e informacionit të ndjeshëm.
Rootkit	Një grup i mjeteve dhe teknikave që fsheh aktivitetin e një programi ose përdoruesi në nivelin e sistemit operativ.	Sigurimi i qëndrueshmërisë së *malware* në sistemin e infektuar, vështirësia e zbulimit.
Dialler	Një program që krijon lidhje telefonike (zakonisht me tarifa të larta) pa dijeninë e përdoruesit, duke përdorur modemët për të kryer telefonata të shtrenjta.	Mund të rezultojë në faturime të larta telefonike dhe në keqpërdorim të burimeve financiare të viktimës.
Ransomware	Një lloj malware që enkripton të dhënat e viktimës dhe kërkon pagesë (shpesh në formë të kriptovalutave) për t'i rikthyer ato.	Humbja e aksesit në të dhëna kritike, shpenzime financiare për pagesën e shpërblimit ose për përpjekjet për të rikthyer të dhënat pa paguar.
Wiper	Një lloj malware që është krijuar për të shkatërruar të dhënat duke i fshirë ato në mënyrë të pakthyeshme nga disku i viktimës.	Humbja e pakthyeshme e të dhënave, që mund të shkaktojë ndërprerje serioze në operacionet e një infrastrukture apo individi.

2.1 Përgatitja

CSIRT kombëtar

a) Zhvillon dhe mirëmban plane për reagimin ndaj incidenteve siç mund të jenë kodet keqdashëse.

b) Përditëson vazhdimisht indikatorët e kompromentimit në rastet e incidenteve me kod keqdashës.
c) Kryen trajnime *Table-Top-Excercise* (TTX) për analistët e CSIRT mbi kodet keqdashëse, zbulimin dhe reagimin ndaj tyre.
ç) Siguron që mjetet dhe sistemet për zbulimin e programeve keqdashës (*malware*) janë të implementuara në nivel kombëtar.
d) Përcakton personat që do të menaxhojnë incidentin duke përcaktuar për secilin rolet dhe përgjegjësitë në menaxhimin e incidentit.

CSIRT Sektorial

a) Ofron udhëzime për sektorin për t'iu përgjigjur incidenteve të kodeve keqdashës.
b) Siguron që sektori specifik është i pajisur me sisteme mbrojtëse si antivirus, *anti-malware* etj të përditësuar.
c) Kryen trajnime fokusuar në sektorin përkatës dhe stimulon ushtrime mbi gjetjen dhe menaxhimin e incidenteve që lidhen me kodet keqdashëse.
ç) Identifikon dhe siguron asetet kritike në nivel sektori të cilat mund të jenë shënjestër i kodit keqdashës.

CSIRT pranë operatorit

a) Implementon dhe mirëmban sistemet mbrojtëse për pajisjet fundore për sistemet kritike dhe të rëndësishme të infrastrukturës.
b) Kryen përditësimet e programeve për të shmangur dobësitë që mund të shfrytëzohen nga kodi keqdashës.
c) Trajnon stafin me praktikat më të mira për të shmangur infektimet me kod keqdashës, siç mund të jetë ndërgjegjësimi mbi sulmet *phishing.*
ç) Aplikon politika dhe procedura për:
   i. Priviliegjet e përdoruesve
   ii. Fjalëkalimet
   iii. Përdorimin e programeve, shkarkimin dhe ekzekutimin e skedarëve në paisje.
d) Ruan kopje rezervë të sistemeve (*backups*) në mënyrë të vazhdueshme, për të rikthyer shërbimet në rast incidenti.

2.2 Zbulimi

CSIRT Kombëtar

a) Monitoron rrjetin kombëtar për aktivitete jonormale që japin indicie për kod keqdashës.
b) Përdor mjete dhe teknika të avancuara për të zbuluar kërcënime apo anomali, dhe mjedise testimi për identifikimin e kodeve keqdashëse.
c) Rakordon të dhënat me burime të ndryshme informacioni si CSIRT-i sektorial dhe CSIRT-i pranë operatorit për të gjetur më tej shpërndarjen e mundshme të infektimit.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit me qëllim implementimin e mjeteve për zbulimin, analizimin dhe vëzhgimin e kodit keqdashës.

b) Shpërdan njoftimet e rëndësishme të zbuluara me CSIRT-in kombëtar dhe CSIRT-et e tjera sektoriale me qëllim koordinimin ndaj reagimit.

CSIRT pranë operatorit

a) Përdor mjetet e zbulimit dhe reagimit (EDR) për të monitoruar për shenja të kodit keqdashës në sisteme.
b) Monitoron çdo përpjekje për lidhjet në rrjet që vijnë si rrjedhojë e kodit keqdashës. Shikon për IP që krijojnë komunikime me sistemin duke përdorur mjete apo komanda si: **Task Manager => Performance => Resource monitor**, **tcpview** (Sysinternals Suite), komandën **netstat -ano** për sistemet ***Windows***. Për sistemet ***Linux*** përdor **netstat -tulpn** dhe **netstat -tupn**, ose çdo mjet apo komandë tjetër që operatori zotëron për monitorimin e aktiviteteve keqdashëse.
c) Monitoron për procese të dyshimta përmes **Task Manager** ose **Procexp (**Sysinternals Suite**)** në sistemet ***Windows*** dhe me komandat **htop** ose **ps -ef** në sistemet ***Linux***
ç) Vëzhgon për çdo skedar të krijuar ose modifikuar nga malware (kryesisht në direktorinë TEMP për formatin .**exe**, **ps1**, **vbs** etj. për sistemet *Windows* – në direktorinë **tmp** për skedarë **.py**, **sh** për sistemet *Linux*).
d) Përdor Thor Lite për Yara Rules ose implementon Yara Rules manualisht në *Firewall*, për zbulimin e skedarëve të tjerë keqdashës në sistem.
dh) Shënon IP-të dhe skedarët e zbuluara si shenja të kompromentimit (IoCs).
e) Kontrollon për përdorues të shtuar, nëpërmjet komandës **lusrmgr.msc** (***Windows***) ose komandës cat /etc/passwd (***Linux***), si dhepër përdoruesit e domain, shikohet pema e përdoruesve në *Active Directory.*
ë) Raporton menjëherë çdo zbulim të kodit keqdashëse drejt CSIRT-it kombëtar dhe atij sektorial.

2.2.1 Zbulimi për rastet ransomware

CSIRT Kombëtar

a) Monitoron në mënyrë të vazhdueshëme trafikun për të zbuluar sjellje të njohura të *ransomware*, si enkriptimi i të dhënave dhe kërkesa të shtuara për trafik me shërbime të jashtme.
b) Përdor sisteme të avancuara të zbulimit dhe platforma inteligjente që ndihmojnë në evidentimin e rasteve të *ransomware* si dhe komunikimet me serverat e kontrollit (C2).
c) Monitoron aktivitetet e logimit përmes protokollit (RDP) ose të programeve me lidhje në distancë (teamviewer, anydesk etj) për të zbuluar anomali që mund të lidhen me ransomware.
ç) Monitoron për dukuri si kompromentim masiv i skedarëve ose procese që tentojnë të enkriptojnë të dhëna.

CSIRT Sektorial

a) Përdor mjete për zbulimin e tentativave për të enkriptuar të dhëna.
b) Përdor teknika siç është *honeypot* në sektor për të stimuluar sisteme vulnerablël, me qëllim evidentimin e aktiviteteve jonormale në rrjet.

c) Koordinohet me CSIRT-in pranë operatorit për shkëmbimin e indikatorëve të kompromentimit (IOC) të lidhura me ransomwaret e fundit.

CSIRT pranë operatorit

a) Monitoron sistemet për çdo përpjekje të papritur për enkriptim të skedarëve ose fshirje të papritur të kopjeve rezervë (*backups*), duke përdorur mjete të menaxhimit të sistemeve fundore (EDR).
b) Kontrollon për ndryshime në shërbimet e sistemit, si për shembull çaktivizimi i shërbimeve kritike të sigurisë (*antivirus, firewall*).
c) Kontrollon për krijimin e dosjeve të reja të papritura me emra si **"README.txt"** ose **"DECRYPT_INSTRUCTIONS.html,".**
ç) Monitoron lidhjet në rrjet për çdo përpjekje për komunikim me adresat IP ose me domain-e që shërbejnë si servera të kontrollit të ransomware (C2).
d) Vëzhgon për çdo skedar të krijuar ose modifikuar nga malware.
dh) Përdor **Thor Lite** për **Yara Rules** ose implementon Yara Rules manualisht në *Firewall*, për zbulimin e skedarëve të tjerë keqdashës në sistem
e) Shënon IP-të dhe skedarët e zbuluara si shenja të kompromentimit **(IoCs).**

2.3 Identifikimi i incidentit

CSIRT-i Kombëtar

a) Konfirmon prezencën e kodit keqdashës përmes analizës së thelluar, duke shfrytëzuar burimet kombëtare të inteligjencës.
b) Identifikon shtrirjen dhe ndikimin e mundshëm të incidentit në të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit.
c) Njofton CSIRT-in sektorial dhe CSIRT-in pranë operatorit për të identifikuar incidentin e kodit keqdashës.

CSIRT-i Sektorial

a) Koordinohet me CSIRT-in pranë operatorit lidhur me raportimin e incidentit të kodit keqdashës.
b) Ofron informacione për incidentin drejt CSIRT-it kombëtar për analizë të mëtejshme.
c) Asiston operatorët për të gjetur origjinën dhe pikën hyrëse të kodit keqdashës.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton incidentin duke përfshirë llojin e kodit keqdashës dhe sistemet e prekura.
b) Ruan sistemin(et) e prekura për analizim të mëtejshëm duke përfshirë:

i. Log-e (event logs, audit logs, log-e nga sistemet e mbrojtjes etj.),
ii. klon të instancës së kompromentuar.
iii. kopje të skedarit keqdashës në një dosje zip të mbrojtur me fjalëkalim (nëse klonimi i sistemit nuk është i mundur).

c) Përdor komandën **"Get-FileHash"** në **PowerShell** (Windows) ose "**sha256sum**" (Linux) për të marrë vlerën e hash SHA-256 të skedarit keqdashës të zbuluar.

ç) Kontrollon për prezencën e programeve/skripteve/kodeve keqdashëse që ekzekutohen menjëherë pas nisjes së sistemit:

i. Vlerat e regjistrave si:
   - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
   - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

ii. **Autoruns/Autoruns64** (Sysinternals Suite), **Run > shell:startup**, **Task Manager > Startup** dhe tasket e programuara (***Task Scheduler***) për sistemet ***Windows*** dhe komandat **crontab -l**, **ls /etc/cron.*** për sistemet *Linux*

d) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial me informacione të detajuara si loge apo vlerësim paraprak të ndikimit.

dh) Ndan të dhënat me CSIRT-in kombëtar apo atë sektorial në kuadër të procesit të identifikimit të incidentit.

2.3.1 Identifikimi për rastet ransomware

CSIRT Kombëtar

a) Verifikon praninë e ransomware përmes analizave të thelluara nga informacionet dhe të dhënat e vendosura në dispozicion nga CSIRT-i pranë operatorit dhe CSIRT-i sektorial si dhe përdor inteligjencën e sigurisë kombëtare për të identifikuar sulmuesin dhe vektorin e sulmit.

b) Përpunon raportet e incidenteve të paraqitura nga CSIRT-i sektorial dhe ai pranë operatorit, duke krijuar një hartë të shtrirjes së mundshme të ransomware në infrastrukturën kritike dhe të rëndësishme në nivel kombëtar.

c) Njofton CSIRT-in sektorial dhe CSIRT-in pranë operatorit për identifikimin e variantit të ransomware, duke përfshirë dhe indikatorët e kompromitimit (IoCs) për të lehtësuar masat mbrojtëse.

CSIRT Sektorial

a) Mbledh dhe siguron informacione të sakta për CSIRT-in kombëtar, duke përfshirë të dhëna mbi llojin e ransomware dhe mënyrën e shpërndarjes në sektor.

b) Punon ngushtë me operatorët për të identifikuar pikën fillestare të infektimit dhe metodat e përdorura për të shmangur masat e sigurisë.

CSIRT pranë operatorit

a) Dokumenton incidentin duke identifikuar llojin e ransomware, shenjat e para të infektimit dhe sistemet e prekura.

b) Siguron ruajtjen e provave, duke përfshirë:

i. Mbledhjen e log-eve të rëndësishme nga sistemet e prekura.

ii. Krijimin e një kloni të instancës së kompromentuar për analizë të mëtejshme, duke u siguruar që sistemi origjinal të ruhet i paprekur.

iii. Ruajtjen e skedarit të ransomware në një dosje të kompresuar dhe të mbrojtur me fjalëkalim,

c) Raporton të dhëna të detajuara mbi incidentin, duke përfshirë log-e, kopjen e instancës, kopje të skedarëve të identifikuar dhe një vlerësim paraprak të ndikimit tek CSIRT-i kombëtar dhe ai sektorial.

2.4 Komunikimi dhe koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit.
b) Komunikon me autoritetet ligj zbatuese për një koordinim më efikas në zgjidhjen e problemit.
c) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
ç) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT Sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

2.5 Regjistrimi

CSIRT kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidenteve bashkë me detajet rreth incidentit.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit në mbledhjen e informacionit të nevojshëm rreth incidentit.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur nga incidenti me qëllim regjistrimin e incidentit në platformën e menaxhimit të mundësuar nga CSIRT-i kombëtar dhe siguron që të gjithë operatorët e prekur të jenë të përfshirë në procesin e regjistrimit.
b) Mbledh dhe dërgon të dhënat mbi incidentin drejt CSIRT-it kombëtar, duke qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton hapat e ndërmarra për menaxhimin e incidentit dhe e rregjistron atë në platformën e menaxhimit të incidentit në përputhje me përcaktimet e rregullores për kategorizimin e incidenteve të sigurisë kibernetike.
b) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial.

2.6 Kategorizimi i incidentit

CSIRT kombëtar

a) Kategorizon incidentin si kod keqdashës ose *ransomware* bazuar në analizimin dhe zbulimin e kërcënimit.
b) Klasifikon incidentin sipas ndikimit në sigurinë kombëtare, sigurinë publike dhe infrastrukturën kritike.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit mbi kategorizimin dhe jep rekomandimet e nevojshme.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit si kod keqdashës ose *ransomware* dhe ndikimet që ky incident ka në sistemet e tyre si dhe e komunikon atë brenda sektorit përkatës.
b) Ndihmon në përcaktimin e natyrës specifike të kodit keqdashës (p.sh., virus, worm, trojan etj).

CSIRT pranë operatorit

a) Kategorizon dhe raporton incidentin si kod keqdashës ose ransomware duke u siguruar që janë dokumentuar edhe detajet.
b) Merr masa të menjëherëshme për zbutjen e ndikimit dhe mos përhapjen e mëtejshëme të aktivitetit keqdashës.

2.7 Prioritizimi i incidentit

CSIRT Kombëtar

a) Vlerëson kritikalitetin e kodit keqdashës bazuar në ndikimin dhe ndalimin e mundshëm të shërbimeve në nivel kombëtar.
b) Prioritizon reagimin ndaj incidentin bazuar në ashpërsinë dhe shtrirjen e ndikimit për gjitha infrastrukturat kritike dhe të rëndësishme të informacionit.
c) Koordinon menaxhimin e incidentit bazuar në përmbajten me ndikimin më të lartë.

CSIRT Sektorial

a) Vlerëson ndikimin e incidentit në bazë të shërbimeve specifike të sektorit dhe i prioritizon ato.
b) Koordinohet me CSIRT-it pranë operatorit me qëllim prioritizimin e incidentit duke u siguruar që reagimi ndaj incidentit të jetë në të njejtën linjë.

c) Asiston CSIRT-in pranë operatorit me qëllim uljen e nivelit të kërcënimeve në shërbimet operacionale e sektorit.

CSIRT pranë operatorit

a) Vlerëson ndikimin e kodit keqdashës në shërbimet operacionale me fokus në shërbimet kritike.
b) Prioritizon masat mbi reagimin ndaj incidentit dhe rikthen fillimisht sistemet më kritike dhe që kanë nivel risku më të lartë.
c) Raporton vendimet mbi prioritizimin e incidentit drejt CSIRT-it kombëtar dhe atij sektorial bazuar në analizime dhe arsyetime të sakta.

2.8 Analizimi incidentit

CSIRT Kombëtar

a) Kryen analizën forensike të indikatorëve dhe të gjitha të dhënave të vendosura në dispozicion nga CSIRT-i pranë operatorit ose CSIRT-i sektorial, për të kuptuar origjinën, sjelljen apo ndikimin potencial që kodi keqdashës ka.
b) Bashkëpunon me partnerët dhe ekspertët ndërkombëtare për sigurinë kibernetike duke mbledhur më tepër informacion mbi kodet keqdashëse.
c) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në reagimin ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në analizimin e detajuar të incidentit që lidhet me kodin keqdashës.
b) Analizon dobësitë e sektorit të shfrytëzuara për të implementuar kodin keqdashës.
c) Vendos në dispozicion të CSIRT-it kombëtar dhe atij pranë operatorit të dhëna që shërbejnë për të kuptuar më tej rreth situatës.

CSIRT pranë operatorit

a) Analizon incidentin në nivel operacional për të kuptuar cila është pika hyrëse, si është shpërndarë kodi keqdashës dhe sistemet e prekura.
b) Analizon aktivitetin e përdoruesit të kompromentuar dhe shikon nëse ka lëvizje laterale në rrjet.
c) Shpërndan analizë të detajuar me CSIRT-in kombëtar dhe atë sektorial duke ndihmuar në kuptimin e incidentit.
ç) Përdor gjetjet për të përmirësuar mbrojtjen në të ardhmen nga incidente të ngjashme.

2.8.1 Analizimi për rastet ransomware

CSIRT kombëtar

a) Kryen një analizë duke krahasuar me rastet e mëparshme të ransomware, për të kuptuar nëse ky sulm përmban ndonjë element të ri që kërkon trajtim të veçantë.

b) Përdor mjedise të kontrolluara **(sandbox)** për të ekzekutuar dhe analizuar ransomware-in, duke studiuar sjelljen e tij, mekanizmat e enkriptimit dhe mënyrën e përhapjes në sistem.
c) Identifikon të gjitha skedarët dhe proceset e krijuara nga ransomware, duke përdorur teknikën e analizës së memorjes (***memory forensics****, të vendosura në dispozicion nga operatorët*) për të nxjerrë skedarët binarë dhe të dhënat e enkriptuara të krijuara nga malware.
ç) Shikon nëse ekziston një çelës për ti bërë skedarët të aksesueshëm sërisht.
d) Koordinohet me partnerët ndërkombëtar për të arritur në zgjidhjen e incidentit.
dh) Shpërndan rezultatet e analizës me CSIRT-in sekorial dhe atë pranë operatorit për të ndihmuar në parandalimin e incidenteve të ngjashme në të ardhmen.

CSIRT sektorial

a) Harton një raport të detajuar të analizës për sektorin përkatës mbi bazën e raportimeve nga operatorët me qëllim përcaktimin e ndikimit dhe shtrirjen e ransomware, raport të cilin e ndan me CSIRT-in kombëtar dhe atë pranë operatorit.
b) Analizon log-et dhe aktivitetet e rrjetit në sektor për të përcaktuar vektorin fillestar të sulmit dhe përhapjen e ransomware në infrastrukturë.
c) Analizon mesazhet ku kërkohet shpërblim për ransomware-it (***ransom note***) për të identifikuar variantin dhe për të mbledhur informacion të mëtejshëm për metodat e kontaktit dhe qëllimet e sulmuesve.

CSIRT pranë operatorit

a) Analizon aktivitetet e përdoruesve dhe të proceseve gjatë kohës së incidentit për të identifikuar se cilët përdorues ishin të kompromentuar dhe nëse ransomware-i ka arritur të fitojë privilegje të larta në sistem.
b) Përgatit një raport të detajuar mbi ndikimin e ransomware-it në sistemet e tij, duke përfshirë shërbimet e çaktivizuara, dhe ndërprerjet e operacioneve, dhe e ndan këtë informacion me CSIRT-in kombëtar
c) Kryen analizën e disqeve për të identifikuar sektorët e modifikuar ose të enkriptuar nga ransomware dhe për të vlerësuar mundësinë e rikthimit të të dhënave nga kopjet rezervë ose mjetet e rikuperimit të të dhënave.

2.9 Izolimi dhe fshirja kombëtar CSIRT

a) Ofron udhëzime dhe suport teknik për të fshirë kodin keqdashës të evidentuar në nivel kombëtar.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar strategji të qëndrueshmërisë kibernetike për mbrojtjen e sistemeve dhe shërbimeve në të gjithë sektorët.
c) Asiston CSIRT-in pranë operatorit në procesin e fshirjes, duke siguruar që kodi keqdashës të hiqet plotësisht nga të gjitha sistemet e prekura.

CSIRT Sektorial

a) Ndërmerr hapa për izolimin e shpejtë të sistemeve të prekura në sektor, bazuar në

prioritizim, për të parandaluar përhapjen e mëtejshme të ransomware.

b) Asiston CSIRT-in pranë operatorit duke u siguruar që procesi i fshirjes të jetë efektiv.
c) Monitoron situatën për të parandaluar rishfaqjen e kodit keqdashës pasi ajo është fshirë.

CSIRT pranë operatorit

a) Izolon menjëherë sistemet që përmbajnë kodin keqdashës duke shmangur levizjen laterale.
b) Bllokon të gjithë indikatorët e kompromentimit të evidentuara gjatë analizimit ose të raportuara nga CSIRT-i kombëtar apo ai sektorial.
c) Ndjek procedurat që ofrohen nga CSIRT-i- kombëtar dhe ai sektorial, duke siguruar që sistemet janë pastruar nga kodet keqdashëse.
ç) Verifikon që kodi keqdashës është fshirë dhe e raporton statusin drejt ekipeve përkatëse të CSIRT-it komëtar dhe atij sectorial.

2.9.1 Izolimi dhe fshirja për rastet ransomware

CSIRT Kombëtar

a) Kërkon menjëherë izolimin e sistemeve të prekura nga rrjeti kombëtar sapo të jetë identifikuar një sulm ransomware, për të parandaluar përhapjen laterale në infrastrukturën kritike dhe të rëndësishme të informacionit.
b) Koordinon me CSIRT-et-sektoriale dhe ato pranë operatorëve për të zbatuar strategji të përbashkëta izolimi, duke përfshirë ndërprerjen e komunikimeve me serverat e komandës dhe kontrollit (C2) dhe bllokimin e adresave IP të njohura të sulmuesve.
c) Kërkon çaktivizimin e përdoruesve të kompromentuar dhe për të kufizuar qasjen vetëm në inpersonelin e autorizuar për analizim dhe rikthim të sistemit.
ç) Mban një inventar të të gjithë sistemeve të izoluara, duke dokumentuar kohën e izolimit dhe duke ndjekur procedurat për sigurinë e provave digjitale për analizë të mëtejshme.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në përmbushjen e udhëzimeve të CSIRT-it kombëtar për izolimin e sistemeve në sektor, me qëllim që çdo sistem i kompromentuar të shkëputet nga rrjeti sektorial për të shmangur përhapjen e ransomware.
b) Asiston CSIRT-in pranë operatorit lidhur me përdorimin e mjeteve të sigurisë së rrjetit si antivirusi, EDR dhe skanues specifik për ransomware për të krijuar zonat e kufizuara (*quarantine zones*) ku do të vendosen sistemet e prekura për analizim të mëtejshëm, duke ndërprerë të gjitha lidhjet me rrjetin e jashtëm.
c) Asiston CSIRT-in pranë operatorit për të analizuar sistemet e izoluara për të përcaktuar nëse është i mundur fshirja selektive e skedarëve të kompromentuar ose nëse është i nevojshëm një rikthim i plotë i sistemit nga kopjet rezervë.

CSIRT pranë operatorit

a) Izolon menjëherë sistemet e prekura sapo të evidentojë aktivitetin e ransomware, duke ndërprerë të gjitha lidhjet e rrjetit dhe duke çaktivizuar aksesin e përdoruesve për të parandaluar përhapjen e mëtejshme.
b) Përdor mjetet e sigurisë (firewall, EDR) për të bllokuar trafikun drejt dhe nga adresat IP ose domain-et e njohura si servera të komandës dhe kontrollit (C2) të ransomware.
c) Fshin skedarët e identifikuar si të kompromentuar.

d) Krijon një klon të sistemit të prekur para fshirjes për të ruajtur provat digjitale për analizë të mëtejshme, duke dokumentuar të gjitha ndryshimet e bëra në procesin e izolimit dhe fshirjes.
e) Dokumenton të gjitha veprimet e izolimit dhe fshirjes si dhe i raporton ato tek CSIRT-i kombëtar dhe ai sektorial, duke përfshirë detajet e skedarëve të fshirë.

2.10 Rikthimi shërbimeve / të dhënave

CSIRT Kombëtar

a) Asiston CSIRT-in sektorial dhe atë pranë operatorit në rikthimin në gjendje normale të shërbimeve kritike pas incidentit.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit që të gjitha shërbimet e prekura të rikthehen në gjendje pune.
c) Monitoron sistemet pas rikthimit të tyre duke siguruar stabilitet dhe për të shmangur incidentet në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në rikthimin e shërbimeve sipas sektorëve përkatës duke prioritizuar shërbimet bazuar në ato që janë prekur më tepër.
b) Komunikon statusin e rikthimit dhe problematikat e hasura tek CSIRT-I kombëtar dhe palët e treta.

CSIRT pranë operatorit

a) Rikthen shërbimet e prekura nga aktiviteti i kodit keqdashës, duke ndjekur hapat e planit të rekuperimit.
b) Për rastet *ransomware* nëse dekriptimi është i pamundur, rikthehen kopjet rezevë duke u siguruar që nuk janë të infektuara.
c) Vërteton integritetin dhe funksionalitetin e shërbimeve të rikthyera përpara se të rifillojnë operacionet normale
ç) Raporton progresin e rikthimit të shërbimeve dhe çdo problematikë drejt CSIRT- it kombëtar dhe dhe atij sektorial.

2.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport të detajuar rreth kodit keqdashës, veprimet e reagimit ndaj incidentit dhe rezultatet.
b) Kryen një analizë pas incidentit për të nxjerrë mësime për të identifikuar se cilat janë fushat ku ka më tepër nevojë për përmirësim.
c) Ndan raportet me CSIRT-in-sektorial dhe atë pranë operatorit për të përmirësuar reagimin ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Harton një raport për sektorët specifik mbi ndikimin e incidentit, hapat e ndërmarrë për menaxhimin e incidentit dhe përfundimet.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke kontribuar në njohuri specifike për sektorin.
c) Ndan raportet dhe mësimet e nxjerra brenda sektorit për të përmirësuar reagimin ndaj incidenteve në të ardhmen.

CSIRT pranë operatorit

a) Harton një raport përfundimtar me informacionet mbi ndikimin e incidentit dhe rikthimin e shërbimeve.
b) Merr pjesë në procesin e mësimeve të nxjerra duke identifikuar çfarë mund të ishte bërë më mirë gjatë përgjigjes ndaj incidentit.
c) Aplikon rekomandimet për të përmirësuar mbrojtjen ndaj incidenteve mbi kodet keqdashëse.

3) Mbledhja e informacionit

Me mbledhje informacioni do te nënkuptojmë, tentativat aktive dhe pasive që aktorët keqdashës ndërmarrin për të mbledhur të dhëna të ndjeshme ose për të identifikuar dobësi në sistem. Teknikat e përdorura për mbledhjen e informacionit përfshijnë **inxhinierinë sociale**, ku sulmuesit përpiqen të mashtrojnë personelin për të nxjerrë të dhëna konfidenciale, **skanimi i rrjetit**, ku aktorët keqdashës kryejnë analiza të rrjetit dhe shërbimeve për të identifikuar pikat e dobëta dhe portat e hapura. Mënyrë pasive për mbledhjen e informacionit është përmes **mjeteve OSINT (*Open Source Intelligence*)** që i lejon sulmuesit të mbledhin të dhëna nga rrjetet sociale, databazat publike dhe burime të tjera të hapur.

3.1 Përgatitja

CSIRT Kombëtar

a) Zhvillon dhe mirëmban politika dhe udhëzime mbi aktivitetet për mbledhjen e informacionit.
b) Implementon mjete dhe teknologji të avancuara që kryejnë skanim dhe zbulim të vazhdueshëm të cenueshmërisë.
c) Kryen trajnime të rregullta mbi aspektet etike dhe ligjore rreth aktiviteteve të skanimit dhe inxhinierisë sociale.
ç) Krijon një sistem të centralizuar për mbledhjen e të dhënave duke siguruar ruajtjen e sigurt të tyre.
d) Përcakton personat që do të menaxhojnë incidentin duke përcaktuar për secilin rolet dhe përgjegjësitë në menaxhimin e incidentit.

CSIRT Sektorial

a) Krijon një inventar për informacionin që është publik dhe që lidhet me sektorin, si p.sh. adresat IP, domain-et, kontaktet e publikuara dhe aplikacionet e përdorura, të dhënat që aktorët keqdashës mund të shfrytëzojnë.
b) Asiston CSIRT-in pranë operatorit në implementimin e sistemeve të monitorimit për aktivitetet e inxhinierisë sociale, si përpjekjet për phishing dhe mashtrime të tjera, për të identifikuar dhe paralajmëruar për kërcënimet që synojnë mbledhjen e informacionit.
c) Trajnon personelin e sektorit për të njohur teknikat e avancuara të mbledhjes së informacionit nga aktorët keqdashës, si p.sh. skanimi i rrjetit dhe inxhinieria sociale
ç) Teston dhe forcon kontrollet e aksesit në burimet e brendshme të informacionit për të parandaluar aktorët keqdashës dhe personat të pautorizuar që të kenë akses në informacione të ndjeshme.
d) Krijojnë një databazë me indikatorët e kompromentimit (IoCs) si janë IP që skanojnë që lidhen me aktivitetet e mbledhjes së informacionit.

CSIRT pranë operatorit

a) Hartojnë dhe zbatojnë politika të brendshme për të mbrojtur të dhënat e ndjeshme dhe për të kufizuar informacionin që është i aksesueshëm publikisht, duke përfshirë detajet si IP e rrjetit të brendshëm, kontaktet dhe sistemet e brendshme.
b) Identifikojnë dhe kontrollojnë të gjitha informacionet e publikuara nga infrastruktura, duke përfshirë faqet e internetit, rrjetet sociale dhe dokumentet publike, për të reduktuar të dhënat që mund të përdoren nga aktorët keqdashës për qëllime të mbledhjes së informacionit.
c) Kryejnë trajnime të rregullta për stafin për të njohur taktikat e inxhinierisë sociale, siç janë *phishing* dhe *vishing* (phishing në telefon), dhe për t'i udhëzuar ata mbi mënyrat e raportimit të menjëhershëm të këtyre përpjekjeve te ekipi i sigurisë.
ç) Implementojnë masa mbrojtëse për aksesin e sistemeve dhe shërbimeve të brendshme, duke përdorur autentifikim shumëfaktorësh (MFA) dhe kufizimin e qasjes për personat e paautorizuar, për të minimizuar mundësinë që aktorët keqdashës të mbledhin informacion.
d) Skanojnë rregullisht rrjetin dhe sistemet e tyre për të identifikuar dhe adresuar dobësitë që mund të shfrytëzohen nga sulmuesit për mbledhjen e informacionit.

3.2 Zbulimi

CSIRT Kombëtar

a) Monitoron trafikun në nivel kombëtar për të identifikuar aktivitete të skanimit nga IP të panjohura ose të dyshimta të cilat analizohen përmes platfomave inteligjente.
b) Kryen kërkime të vazhdueshme në internet për gjetjen e informacioneve të ndjeshme që mund të shfrytëzohen nga aktorët keqdashës dhe raportohen drejt CSIRT-it pranë operatorit dhe atij sektorial.
c) Koordinohet me institucionet e tjera kombëtare dhe ndërkombëtare për të identifikuar burimet e përpjekjeve të mbledhjes së informacionit dhe për të ndarë indikatorët e kompromentimit (IoCs).
ç) Rakordon të dhënat e skanimeve me burime të ndryshme informacioni siç janë platformat e inteligjencës.

CSIRT Sektorial

a) Kordinohet me CSIRT-in pranë operatorit me qëllim implementimin në sektorin përkatës të mekanizmave të nevojshme lidhur me zbulimin e aktivitetit skanues të cilat mund të kenë synim sisteme kritike.
b) Shpërndan indikatorët e skanimeve të zbuluara nga CSIRT pranë operatorit drejt CSIRT-it-kombëtar dhe CSIRT-eve të tjerë sektorial.
c) Ka qasje proaktive në monitorim dhe analizimin e skanimeve për të kuptuar kërcënimet e mundshme.

CSIRT pranë operatorit

a) Përdor mjetet e monitorimit të rrjetit për të zbuluar aktivitet të paautorizuar ose të dyshimtë për skanim ose tentativa për inxhinieri sociale.
b) Raporton menjëherë aktivitetet e skanimeve drejt CSIRT-it kombëtar dhe atij sektorial.
c) Implementon mjete të brendshme për të monitoruar trafikun e rrjetit dhe për të identifikuar kërkesa të shumta DNS, ARP, ose aktivitete të tjera që mund të tregojnë për një përpjekje të përgjimit të trafikut brenda infrastrukturës.
ç) Mbledh informacion mbi aktivitetet e dyshimta dhe e ndan menjëherë me CSIRT-in sektorial për një reagim të koordinuar dhe për të ndihmuar në përcaktimin e shtrirjes së tentativës për mbledhje informacioni.
d) Ruan log-et dhe të dhënat e lidhura me aktivitetin keqdashës për investigim të mëtejshëm.

3.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Konfirmon prezencën e aktivitetit të mbledhjes së informacionit si pjesë e një incidenti të mundshëm sigurie përmes analizës fillestare pas zbulimit të aktivitetit keqdashës.
b) Analizon dhe vlerëson raportet e aktiviteteve të phishing dhe inxhinierisë sociale të raportuara nga CSIRT-pranë operatorit dhe ai sektorial, për të identifikuar taktika të reja që mund të përdoren për mbledhjen e informacionit
c) Identifikon shtrirjen dhe ndikimin kryesisht në të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit.
ç) Njofton CSIRT-in sektorial dhe atë pranë operatorit rreth incidentit të identifikuar dhe ndikimit të tij.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit lidhur me raportimin e incidentit të cilësuar si "mbledhje informacioni" të bërë nga vetë operatorit për të përcaktuar nëse paraqet kërcënim për asetet e tyre në shkallë më të gjërë.
b) Koordinohet me CSIRT-in pranë operatorit për të vlerësuar ndikimin e skanimit brenda sektorit përkatës.
c) Ofron informacion të detajuar për incidentin drejt CSIRT-it kombëtar për një analizë më të thelluar.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton incidentin duke përfshirë burimin e sulmit, përdoruesit dhe sistemet e shënjestruara, dhe nivelin e privilegjeve të përdoruesit.
b) Analizon log-et e sistemit dhe të rrjetit për të identifikuar burimet e aktivitetit të dyshimtë, si: adresat IP që kërkojnë të mbledhin informacion përmes skanimit të portave.
c) Shikon përmbajtjen e mesazheve të dyshimta në postën elektronike dhe identifikon nëse kemi incident apo tentativë të inxhinierisë sociale dhe përcakton objektivat e aktorëve keqdashës bazuar në marrësin e mesazheve.
ç) Monitoron log-et e serverave dhe të aplikacioneve për të identifikuar nëse ndonjë shërbim është përdorur për të grumbulluar informacioni nga jashtë, si për shembull kërkesat e shumta për informacion nga një adresë IP e vetme.
d) Mbledh dhe dokumenton informacionin e identifikuar, duke përfshirë adresat IP, teknikat e përdorura, dhe skedarët e dyshimtë, dhe i raporton ato menjëherë tek CSIRT-i kombëtar dhe ai sektorial për analizë dhe koordinim të mëtejshëm

3.4 Komunikimi dhe Koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe atij pranë operatorit.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e incidentit.

CSIRT Sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me CSIRT-in pranë operatorit për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

3.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidenteve dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.

b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit në mbledhjen e informacionit të nevojshëm rreth incidentit bazuar në dokumentacion.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur nga incidenti me qëlim regjistrimin e incidentit në platformën e menaxhimit të incidenteve.
b) Koordinohet me operatorët e infrastrukturave të prekur nga incidenti me qëllim që të jenë të përfshirë në procesin e regjistrimit të incidentit.
c) Mbledh dhe dërgon të dhënat mbi incidentin drejt CSIRT-it kombëtar, duke qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton incidentin e skanimit dhe gjetjet bazuar në të dhënat e mbledhura.
b) Regjistron incidentin në përputhje me përcaktimet e rregullores së kategorizimit të incidentit të sigurisë kibernetike.
c) Raporton incidentin tek CSIRT-i kombëtar dhe ai sektorial.

3.6 Kategorizimi i incidentit

CSIRT Kombëtar

a) Kategorizon incidentin e mbledhjes së informacionit si skanim, inxhinieri sociale, OSINT etj bazuar në natyrën, shtrirjen dhe ndikimin potencial në sigurinë kombëtare.
b) Klasifikon incidentin sipas ndikimit dhe qëllimin që fshihet pas mbledhjes së informacionit dhe sistemet e shënjestruara.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit mbi kategorizimin dhe jep rekomandimet e nevojshme.

CSIRT Sektorial

a) Kordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit të skanimit brenda sektorit, bazuar në ndikimin e tij dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e aktivitetit të skanimit dhe rëndësinë e tij për shërbimet operacionale e sektorit.

CSIRT pranë operatorit

a) Kategorizon incidentin e mbledhjes së informacionit si skanim, inxhinieri sociale, OSINT.
b) Raporton aktivitetin e mbledhjes së informacionit, duke u siguruar që të gjitha informacionet përkatëse çojnë në kategorizimin e incidentit.
c) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.
ç) Zbaton masa të menjëhershme për të adresuar çdo cënueshmëri të identifikuar përmes aktivitetit të mbledhjes së informacionit.

3.7 Prioritizim i incidentit

CSIRT Kombëtar

a) Vlerëson rëndësinë e aktivitetit të mbledhjes së informacionit bazuar në potencialin e tij për të identifikuar ose shfrytëzuar dobësitë në sistemet kombëtare.
b) Prioritizon përgjigjen ndaj incidentit, duke u fokusuar në ato incidente që mund të çojnë në shkelje të sigurisë.
c) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për tu siguruar që incidentet më kritike të adresohen menjëherë.

CSIRT Sektorial

a) Vlerëson ndikimin e aktivitetit të skanimit në shërbimet kritike specifike të sektorit dhe prioritizon në bazë të kritikalitetit.
b) Koordinohet me CSIRT-in pranë operatorit me qëllim prioritizimin e incidentit duke u siguruar që reagimi ndaj incidentit të jetë në të njejtën linjë.
c) Fokusohet në zbutjen e kërcënimeve duke i kushtuar rëndësi shërbimeve me kritike të prekura nga skanimi.

CSIRT pranë operatorit

a) Vlerëson ndikimin e aktivitetit të mbledhjes së informacionit në proceset operacionale dhe prioritizon veprimet e reagimit ndaj incidentit sipas rëndësisë së shërbimeve.
b) Siguron që dobësitë e identifikuara përmes skanimit të adresohen menjëherë.
c) Raporton vendimet për prioritizimin tek CSIRT-i kombëtar dhe ai sektorial, bazuar në arsyetime të sakta.

3.8 Analizimi incidentit

CSIRT Kombëtar

a) Kryen një analizë të plotë të aktivitetit të skanimit, duke u fokusuar në burimin, qëllimin dhe ndikimin e mundshëm.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë rreth indikatorëve të identifikuar gjatë fazës së analizimit.
c) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në përgjigjet ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Kryen një analizë në nivel sektori mbi aktivitetet për mbledhje informacioni, duke shfrytëzuar informacionin e vendosura në dispozicion nga operatorët dhe platforma e inteligjencës së kërcënimeve.
b) Ofron asistencë në analizimin e burimeve që aktorët keqdashës kanë shfrytëzuar për të mbledhur informacionin dhe sugjeron strategji për eliminimin e këtyre informacioneve nga këto burime.
c) Vendos në dispozicion të CSIRT-it kombëtar të dhëna që shërbejnë për të kuptuar më tej rreth situatës.

CSIRT pranë operatorit

a) Analizon aktivitetin e mbledhjes së informacionit në nivel operativ, duke u fokusuar në mënyrën se si mund të ndikojë në sistemet kritike.
b) Shpërndan gjetjet me CSIRT-in kombëtar dhe atë sektorial për të ndihmuar këto të fundit të kuptojnë më tepër rreth incidentit të skanimit, inxhinierisë sociale etj.
c) Shfrytëzon gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar shfrytëzimin e dobësive të identifikuara.

3.9 Izolimi dhe fshirja

CSIRT kombëtar

a) Ofron udhëzime dhe mbështetje për uljen e ndikimit nga aktivitetet të identifikuara si "mbledhje informacioni".
b) Koordinohet me CSIRT-it sektorial dhe atë pranë operatorit për të siguruar strategji të qëndrueshmërisë kibernetike në të gjithë sektorët.
c) Drejton përpjekjet për të adresuar çdo informacion të ekspozuar nga aktiviteti i mbledhjes së informacionit, duke siguruar eliminimin e këtyre informacioneve.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit me qëllim aplikimin e masave mbrojtëse në të gjithë sektorin për të parandaluar shfrytëzimin e informacioneve të mbledhura.
b) Bashkëpunon me operatorët për të shmangur kërcënimet e mundshme të lidhura me aktivitetin keqdashës.
c) Monitoron situatën për të siguruar që janë marrë masa mbi të gjitha informacionet e ekspozuara.

CSIRT pranë operatorit

a) Izolon menjëherë pajisjet dhe sistemet e identifikuara si të kompromentuara nga rrjeti për të parandaluar përhapjen e mëtejshme të aktiviteteve të mbledhjes së informacionit dhe për të mbrojtur të dhënat e ndjeshme.
b) Bllokon adresat IP, domain-et, dhe burimet e tjera të dyshimta që janë përdorur për mbledhjen e informacionit, duke përdorur rregullat e sistemeve mbrojtëse si: firewall-it dhe IDS/IPS për të parandaluar çdo komunikim të mëtejshëm me aktorët keqdashës.
c) Monitoron në mënyrë aktive sistemet e izoluara për aktivitet të dyshimtë të vazhdueshëm, si përpjekjet e përsëritura për komunikim, duke siguruar se izolimi ka qenë efektiv.
ç) Dokumenton të gjitha veprimet e ndërmarra gjatë fazës së izolimit dhe fshirjes, duke përfshirë adresat IP të bllokuara, skedarët e fshirë, dhe llogaritë e çaktivizuara, dhe e ndan këtë informacion me CSIRT-in kombëtar dhe atë sektorial për një përgjigje të koordinuar dhe analizë të mëtejshme.
d) Ndjek procedurat që ofrohen nga CSIRT-i kombëtar dhe ai sektorial për eliminimin e informacionit sensitiv të ekspozuar duke siguruar që të ndërmerren të gjitha hapat e nevojshëm.

3.10 Rikthimi i shërbimeve / të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e të gjithë shërbimeve të prekur në funksionimin normal.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikthehen plotësisht në gjëndje pune.
c) Monitoron sistemet gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidentet në të ardhmen.

CSIRT Sektorial

a) Ndihmon operatorët në rikuperimin e shërbimeve specifike të sektorit, duke i dhënë përparësi sistemeve më kritike të prekura.
b) Komunikon statusin e rikuperimit dhe situatën në vazhdim drejt CSIRT-it kombëtar dhe palët e interesuara.

CSIRT pranë operatorit

a) Rikthen shërbimet e prekura nga aktiviteti i skanimit, duke ndjekur planet e reagimit ndaj incidentit.
b) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikthyera përpara se të rifillojnë operacionet normale.
c) Raportojnë progresin e rikuperimit dhe çdo sfidë tek CSIRT-i kombëtar dhe ai sektorial për ndihmë të mëtejshme.

3.11 Aktiviteti pas incidentit

CSIRT kombëtar

a) Harton një raport ku përshkruan incidentin për mbledhjen e informacionit, veprimet e reagimit ndaj incidentit dhe rezultatet.
b) Rishikon aktivitetin pas incidentit për nxjerrjen e mësimeve dhe për evidentimin e fushave ku ka nevojë për përmirësim.
c) Përditëson planin për reagim bazuar në mësimet e nxjerra.
ç) Shpërndan raportin me CSIRT-in sektorial dhe atë pranë operatorit për të rritur gatishmërinë e përgjithshme.

CSIRT Sektorial

a) Përgatit një raport për sektorin duke përshkruar ndikimin e aktivitetit të skanimit hapat e reagimit ndaj incidentit dhe përpjekjet për rikuperim.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke kontribuar me njohuri dhe rekomandime specifike të sektorit.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar planin për reagimin ndaj incidenteve në të ardhmen.

CSIRT pranë operatorit

a) Harton një raport përfundimtar me informacion të detajuar mbi ndikimin, reagimin dhe rikuperimin e aktivitetit keqdashës.
b) Angazhohet në procesin e mësimeve të nxjerra, duke identifikuar çfarë mund të përmirësohet për incidentet e ngjashme në të ardhmen.
c) Aplikon rekomandimet për të forcuar mbrojtjen dhe për të përmirësuar aktivitetet e ardhshme të skanimit.

4) Përpjekjet për ndërhyrje

Tentativat për akses të paautorizuar në fushën e sigurisë kibernetike janë shenjat e vazhdueshme të përpjekjeve për të depërtuar në sistemet e një infrastrukture informacioni ose paisjeve të një individi. Këto përpjekje vijnë nga individë apo grupime të paautorizuar që synojnë të përfitojnë qasje të paligjshme në të dhëna sensitive, të shkaktojnë dëme, ose të shfrytëzojnë resurset në mënyrë të paligjshme. Tentativat për ndërhyrje janë në forma të ndryshme si: *email phishing*, *brute-force,* injektimi i kodeve keqdashës (SQLi, XXS) etj.

4.1 Përgatitja

CSIRT Kombëtar

a) Zhvillon dhe mirëmban politika dhe procedura për zbulimin dhe përgjigjen ndaj përpjekjeve për ndërhyrje.
b) Zbaton teknologji të avancuara sigurie, përfshirë sistemet e zbulimit të ndërhyrjeve (IDS) dhe sistemet e parandalimit të ndërhyrjeve (IPS), në të gjithë rrjetet kombëtare.
c) Kryen trajnime të vazhdueshme për analistët e CSIRT për të identifikuar dhe reaguar ndaj përpjekjeve për ndërhyrje.
ç) Bashkëpunon me organizatat globale të sigurisë kibernetike për të qëndruar të informuar mbi taktikat dhe teknikat më të fundit të ndërhyrjes.
d) Përcakton personat përgjegjës për reagimin e incidentit dhe përcakton rolet dhe përgjegjësitë e gjithësecilit.

CSIRT Sektorial

a) Asiston operatorët e infrastrukturave nëpërmjet udhëzimeve për sektorin specifik për monitorimin dhe parandalimin e përpjekjeve të ndërhyrjes.
b) Siguron që rrjetet sektoriale janë të pajisura me teknologji të përditësuara IDS/IPS.
c) Kryen trajnime për ekipet e CSIRT-it sektorial dhe atij pranë operatorit për të identifikuar shenjat e përpjekjes për ndërhyrje.
ç) Bashkëpunon me CSIRT-in pranë operatorit për të zhvilluar një plan për reagimin ndaj incidenteve siç janë përpjekjet për ndërhyrje.

CSIRT pranë operatorit

a) Implementojnë dhe mirëmbajnë sisteme sigurie që monitorojnë trafikun e rrjetit për shenja të tentativave për ndërhyrje.
b) Trajnojë stafin për të njohur aktivitetet e dyshimta dhe për të raportuar përpjekjet e mundshme për ndërhyrje ne sisteme.

c) I vendos stafit të operatorit në dispozicion praktikat më të mira të sigurisë, si kufizimi i qasjes nga përdorues me privilegje të ulëta, siguron që fjalëkalimet plotësojnë standartet, aplikon rregullisht përditësimet, për të reduktuar rrezikun e ndërhyrjeve të suksesshme.
ç) Rishikon dhe përditëson rregullisht konfigurimet e sigurisë për të adresuar kërcënimet e reja.

4.2 Zbulimi

CSIRT Kombëtar

a) Monitoron vazhdimisht rrjetet kombëtare për indikatorë të përpjekjeve për ndërhyrje, si përpjekje për qasje të paautorizuar, trafik i pazakontë dhe sjellje jonormale të sistemit.
b) Përdor burime të inteligjencës së kërcënimeve dhe mjete të zbulimit të anomalive për të identifikuar përpjekjet e mundshme të ndërhyrjes.
c) Bashkëpunon me CSIRT-in sektorial dhe atë pranë operatorit për të rritur kapacitetet për zbulimin e përpjekjeve për ndërhyrje duke ndarë informacion dhe të dhëna mes palëve.

CSIRT Sektorial

a) Bashkëpunon me CSIRT-in pranë operatorit me qëllim implementimin e mekanizmave për zbulimin dhe identifikimin e përpjekjeve të ndërhyrjes që synojnë infrastrukturën kritike.
b) Njofton përpjekjet për ndërhyrje të zbuluara drejt CSIRT-it kombëtar dhe CSIRT-eve të tjera sektoriale për të siguruar një përgjigje të koordinuar.

CSIRT pranë operatorit

a) Përdor mjete për monitorimin e rrjetit për të zbuluar përpjekjet për ndërhyrje të paautorizuara.
b) Monitoron për tentativa të shumta për të fituar qasje në protokollet si: smb, ssh, ftp, http/https, rdp etj.
c) Kryen skanime të brendshme për të evidentuar sisteme apo shërbime që mund të kenë dobësi të njohura që mund të shfrytëzohen nga aktorët keqdashës.
ç) Monitoron aktivitetin e përdoruesve për të evidentuar sjelljet jonormale të tyre, sic janë tentativat për qasje jashtë orarit të punës apo tentativa për të fituar qasje në sekdarë për të cilat nuk është i autorizuar për ti përdorur.
d) Raporton menjëherë çdo përpjekje të zbuluar të ndërhyrjes drejt CSIRT-it kombëtar dhe atij sektorial.
dh) Ruan loget dhe të dhënat e lidhura me përpjekjet për ndërhyrje të zbuluara me qëllim investigimin e mëtejshm.

4.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Kategorizon si incident kibernetik përmes analizës nga të dhënat e mbledhura përpjekjet për ndërhyrje.
b) Verifikon shtrirjen dhe ndikimin e mundshëm të përpjekjes për ndërhyrje në aspektin e sigurisë kombëtare për infrastrukturat kritike dhe të rëndësishme.
c) Njofton përpjekjet për ndërhyrje tek CSIRT-i sektorial dhe ai pranë operatorit për përpjekjet për ndërhyrje dhe pasojat e mundshme të saj.

CSIRT Sektorial

a) Koordinon me CSIRT-in pranë operatorit përpjekjen për ndërhyrje të raportuar nga vet ata si dhe vlerëson ndikimin e saj në asetet specifike të sektorit.
b) Koordinohet me operatorët për të përcaktuar shtrirjen e tentativeës për ndërhyrje brenda sektorit.
c) Jep informacion të detajuar për incidentin drejt CSIRT-it kombëtar për një analizë më të thelluar.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton përpjekjen e ndërhyrjes, duke përfshirë burimin, metodën dhe cilat shërbime apo përdorues janë objektiv.
b) Verifikon nivelin e privilegjeve që ka përdoruesi mbi të cilën po tentohet të fitohet qasje.
c) Në sulmet *phishing*, identifikohen IP e dërguesit, skedari ose lidhja (*link*) që mund të jenë pjese e email-it dhe cilësohen si indikatorë të kompromentimit.
ç) Identifikon IP-të që tentojnë te injektojnë kod keqdashës në sisteme apo shërbime, për të fituar qasje të paautorizuar.
d) Analizon sjelljen e personelit për të identifikuar nëse kemi të bëjmë me persona të brendshëm që fshihen pas tentativave.
dh) Identifikon nëse tentativat për të fituar qasje vijnë nga një sulm zinxhir të cilat prekin fillimisht operatorë të palëve e treta që ofrojnë shërbime drejt infrastrukturave kritike apo të rëndësishme.
e) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial, duke i mundësuar të gjitha të dhënat përkatëse dhe analizën fillestare.
ë) Ndihmon në identifikimin e qëllimit që përpjekjet për ndërhyrje kanë dhe ndikimin e mundshëm në shërbimet operacionale.

4.4 Komunikimi dhe Koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.

b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

4.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron si incident përpjekjet për ndërhyrje në platformën e menaxhimit të incidenteve, duke u siguruar që të gjitha të dhënat e mbledhura të jenë të regjistruara.
b) Koordinon me CSIRT-in sektorial dhe atë pranë operatorit për të mbledhur informacione shtesë dhe për të siguruar që incidenti të jetë dokumentuar plotësisht.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në regjistrimin e incidentit në platformën e menaxhimit të incidenteve dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Dërgon informacionet e mbledhura dhe detajet e incidentit drejt CSIRT-it kombëtar për të qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton përpjekjet për ndërhyrje dhe çdo gjetje fillestare bazuar në të dhënat e mbledhura.
b) Siguron regjistrimin e incidentit sipas përcaktimeve në rregulloren për kategorizimin e incidenteve kibernetike.
c) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial me të gjitha detajet përkatëse.

4.6 Kategorizimi i incidentit

CSIRT Kombëtar

a) Kategorizon si incident përpjekjen për ndërhyrje bazuar në natyrën, shtrirjen dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Klasifikon incidentin sipas ashpërsisë së tij, duke marrë parasysh ndikimin që mund të kenë sistemet e shënjestruara.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin dhe jep udhëzime si të reagojë ndaj incidentit.

CSIRT Sektorial

a) Kordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit të skanimit brenda sektorit, bazuar në ndikimin e tij dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e natyrës të "përpjekjes për ndërhyrje" dhe rëndësinë e saj për operacionet sektoriale.

CSIRT pranë operatorit

a) Kategorizon si incident përpjekjen për ndërhyrje.
b) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.

c) Zbaton masa të menjëhershme për të zbutur çdo dëm të mundshëm të shkaktuar nga përpjekja për ndërhyrje.

4.7 Prioritizim i incidentit

CSIRT Kombëtar

a) Vlerëson kritikalitetin që përpjekjet për ndërhyrje kanë, duke u bazuar në potencialin e saj për të kompromet uar të dhëna të ndjeshme ose për të ndërprerë shërbimet kritike.
b) Prioritizon reagimin ndaj incidentit, duke u fokusuar në ato incidente që mund të çojnë në shkelje të sigurisë në sisteme apo shërbime kritike.
c) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që incidentet më kritike të trajtohen menjëherë.

CSIRT Sektorial

a) Vlerëson ndikimin e përpjekjeve për ndërhyrje në shërbimet kritike të sektorit dhe i prioritizon ato sipas nevojës.
b) Koordinohet me CSIRT-in pranë operatorit për prioritizimin e incidentit, me qëllim për të koordinuar dhe sinkronizuar përgjigjen ndaj incidentit.
c) Asisiton CSIRT-in pranë operatorit në zbutjen e kërcënimeve më kritike të identifikuara përmes incidentit.

CSIRT pranë operatorit

a) Vlerëson ndikimin e përpjekjes për ndërhyrje në proceset operacionale dhe prioritizon veprimet e përgjigjes sipas nevojës.
b) Siguron që çdo dëm potencial ose kompromentim i të dhënave të menaxhohet dhe adresohet menjëherë.
c) Raporton vendimet për prioritizim drejt CSIRT-it kombëtar dhe atij sektorial, duke ofruar analizime dhe arsyetime.

4.8 Analizimi incidentit

CSIRT Kombëtar

a) Kryen analizë të detajuar të përpjekjes për ndërhyrje, duke kuptuar origjinën, metodën, teknikat e aktorëve keqdashës apo ndikimin potencial në sigurinë kombëtare.
b) Përcakton indikatorët e kompromet imit, si IP të dyshimta, hash-e të skedarëve të infektuar, URL-të e dëmshme bazuar në të dhënat e vendosura në dispozicion nga CSIRT-i sektorial dhe ai pranë operatorit.
c) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë që ndihmojnë në reagim ndaj incidentit.
d) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në reagimin ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në analizimin e përpjekjes për ndërhyrje, duke shfrytëzuar informacionet e mbledhura dhe inteligjencën e kërcënimeve.
b) Asiston CSIRT-in pranë operatorit në identifikimin e dobësive të shfrytëzuara nga përpjekja për ndërhyrje dhe sugjeron strategji për zbutjen e dobësive.

c) Vendos në dispozicion të CSIRT-it kombëtar dhe atij pranë operatorit analizime dhe të dhëna që shërbejnë për të kuptuar më tej rreth situatës.

CSIRT pranë operatorit

a) Analizon përpjekjen për ndërhyrje në nivel operativ, duke u fokusuar në mënyrën se si mund të ndikojë në sistemet kritike dhe të dhënat.
b) Shpërndan gjetjet me CSIRT-in kombëtar dhe atë sektorial për të kontribuar në një kuptim më të gjerë rreth incidentit të ndërhyrjes.
c) Zbaton gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar përpjekjet e mëtejshme për ndërhyrje.

4.9 Izolimi dhe fshirja

CSIRT Kombëtar

a) Ofron udhëzime dhe mbështetje për zbutjen e ndikimit të përpjekjeve për ndërhyrje.
b) Koordinon përpjekjet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që strategjitë për qëndrueshmëri kibernetike të zbatohen në të gjitha sektorët.
c) Adreson dobësitë e ekspozuara nga përpjekja për ndërhyrje, dhe jep rekomandime për të ulur numrin e këtyre dobësive.

CSIRT Sektorial

a) Koordinon me CSIRT-in pranë operatorit me qëllim marrjen e masave parandaluese në të gjithë sektorin për të parandaluar shfrytëzimin e mëtejshëm të dobësive.
b) Punon ngushtë me operatorët për të siguruar reduktimin e dobësive që shfrytëzohen për përpjekje për ndërhyrje.
c) Monitoron situatën për të siguruar që të gjitha dobësitë e identifikuara janë adresuar dhe incidenti është zgjidhur plotësisht.

CSIRT pranë operatorit

a) Adreson menjëherë çdo dobësi të identifikuar si "përpjekje për ndërhyrje" si përshembull:
    i. Nëse evidentohen sulme mbi porta e njohura si psh: 21, 22, 3389, filtroni trafikun për këto porta, që të eliminoni sulmet e mundshme.
    ii. Pasi keni identifikuar mësipër IP nga ku vijnë këto tentativa, bllokojini.
    iii. Limitoni tentativat për logim, psh: maksimumi 5 tentativa, dhe më pas përdoruesi të presë 5 minuta.
    iv. Nëse ka dyshime për autentifikimin, ndërmerrni hapa për të rritur mbrojtjen e llogarisë dhe të sistemit. Kjo mund të përfshijë rregullimin e politikave të sigurisë, përdorimin e *note-changes*, deri në bllokimin e llogarive në raste të dyshimta.
b) Ndjek procedurat parandaluese dhe të zbutjes të ofruara nga CSIRT-et, duke siguruar që të gjitha hapat e nevojshëm të ndërmerren si:
    i. Ndryshimi i fjalëkalimeve për përdoruesit apo shërbimet ku është tentuar të fitohet qasje.
    ii. Aplikimi i përditësimeve ose marrja e masave mbi sistemet që kanë dobësi të njohura që çojnë në kompromentim.

c) Verifikon sa efektive kanë qenë masat parandaluese, zbutjen e dobësive dhe e raporton statusin drejt CSIRT-it kombëtar dhe atij sektorial.

4.10 Rikthimi shërbimeve / të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e shërbimeve të prekura nga përpjekja për ndërhyrje.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Monitoron sistemet gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidente e ardhshme.

CSIRT Sektorial

a) Ndihmon në rikthimin e shërbimeve sektoriale, duke prioritizuar shërbimet ose sistemet më kritike të prekura.
b) Mbështet operatorët në rikthimin e shërbimeve në kapacitetet të plotë operacional.
c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim drejt CSIRT-t kombëtar dhe palëve të treta të interesuara.

CSIRT pranë operatorit

a) Rikuperon shërbimet e prekura nga "përpjekjet për ndërhyrje", duke ndjekur planet e rikuperimit të përcaktuara në planin e menaxhimit të incidentit.
b) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikuperuara para se të rifillohen operacionet normale.
c) Raporton progresin e rikuperimit dhe çdo problematikë gjatë procesit drejt CSIRT-it kombëtar dhe atij sektorial për ndihmë të mëtejshme.

4.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport të detajuar në lidhje me përpjekjet për ndërhyrje, veprimet e reagimit ndaj incidentit dhe rezultatet.
b) Kryen rishikim pas incidentit për të identifikuar mësimet e nxjerra dhe ku ka më tepër nevojë për përmirësim.
c) Shpërndan raportet me CSIRT-in sektorial dhe operatorët e infrastrukturës kritike dhe të rëndësishme për të përmirësuar reagimin ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Përgatit një raport për sektorin mbi ndikimin e incidentit, hapat e ndërmarrë për menaxhimin e incidentit dhe përfundimet.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke dhënë rekomadime specifike për sektorin.
c) Shpërndan raportet dhe mësimet e nxjerra brenda sektorit për të përmirësuar reagimin ndaj incidenteve në të ardhmen.

CSIRT pranë operatorit

a) Harton një raport përfundimtar duke ofruar informacion të detajuar mbi ndikimin e incidentit, reagimin ndaj tij dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësime operacionale dhe duke përditësuar planet e reagimit.
c) Zbaton rekomandimet për të forcuar mbrojtjen dhe për të përmirësuar zbulimin për sulmet e ardhshme siç janë përpjekjet për ndërhyrje.

5) Ndërhyrjet

5.1 Përgatitja

CSIRT Kombëtar

a) Zhvillon dhe mirëmban politika dhe procedura për zbulimin dhe përgjigjen ndaj anashkalimit të autentifikimit.
b) Implementon kontrolle të avancuara të sigurisë si autentifikimi me shumë faktorë (MFA), politika të forta të fjalëkalimeve dhe rishikime të vazhdueshme në sistemet kombëtare.
c) Kryen trajnime të rregullta për analistët e CSIRT-eve mbi njohjen dhe reagimin ndaj teknikave të anashkalimit të autentifikimit.
ç) Bashkëpunon me organizata të sigurisë kibernetike për shkëmbimin e informacionit dhe për të qëndruar të informuar mbi metodat e reja të anashkalimit të autentifikimit.
d) Përcakton personat që do të menaxhojnë incidentin duke përcaktuar për secilin rolet dhe përgjegjësitë në menaxhimin e incidentit.

CSIRT Sektorial

a) Koordinon punën me CSIRT-in pranë operatorit nëpërmjet dhënies së udhëzimeve për sektorin specifik për të siguruar mënyrat e autentifikimit në përputhje me standardet kombëtare.
b) Koordinohet me operatorët e infrastrukturave me qëllim implementimin e autentifikimit me shumë faktorë në të gjithë sektorin dhe përditëson rregullisht kontrollet e aksesit.
c) Trajnon ekipet sektoriale të CSIRT-eve për identifikimin, zbutjen dhe shmangien e anashkalimit të autentifikimit.

CSIRT pranë operatorit

a) Aplikon dhe mirëmban mekanizma të fortë të autentifikimit, duke përfshirë MFA, fjalëkalime të forta dhe rishikime të vazhdueshme të aksesit.
b) Trajnon stafin mbi praktikat e sigurta të autentifikimit dhe rëndësinë e raportimit të aktiviteteve të dyshimta.
c) Implementon mjete monitoruese për të zbuluar aktivitete jo të zakonshme të qasjes ose tentative të dështuara për hyrje.
ç) Rishikon dhe përditëson rregullisht politikat e qasjes dhe konfigurimet e autentifikimit.

5.2 Zbulimi

CSIRT Kombëtar

a) Monitoron rrjetin kombëtar për aktivitete të anashkalimit të autentifikimit, si modele të pazakonta të hyrjeve, përpjekje të përsëritura të dështuara për hyrje, ose qasje nga vendndodhje të ndryshme.
b) Përdor mjete për zbulimin e anomalive dhe inteligjencën e kërcënimeve për të identifikuar aktivitete të mundshme të anashkalimit.
c) Përdor platfomra inteligjente për evidentimin e të dhënave që kanë rrjedhur dhe ua përcjell CSIRT -ve përkatës me qëllim shmangien e qasjes së paautorizuar.
ç) Bashkëpunon me CSIRT-et sektoriale dhe ato pranë operatorëve për të përmirësuar kapacitetet e zbulimit përmes njohurive dhe të dhënave të përbashkëta.

CSIRT Sektorial

a) Përdor mjete specifike për sektorin për të zbuluar përpjekjet për anashkalimin e autentifikimit që synojnë sisteme, shërbime apo qasje në zona kritike.
b) Shpërndan informacionin mbi aktivitetet e zbuluara për anashkalimin e autentifikimit me CSIRT-in kombëtar dhe CSIRT-et e tjera sektoriale për të pasur një përgjigje të koordinuar.
c) Asiston operatorët me qëllim monitorimin e vazhdueshëm për dobësi që mund të shfrytëzohen për të anashkaluar autentifikimin në shërbimet që ofrohen përmes ndërfaqes publike në internet.
ç) Koordinohet me CSIRT-in pranë operatorëve me qëllim monitorimin e sistemeve të autentifikimit për aktivitete të pazakonta që mund të tregojnë shenja të anashkalimit të autentifikimit.

CSIRT pranë operatorit

a) Monitoron rrjetet dhe sistemet për të zbuluar përpjekje të paautorizuara për hyrje dhe shenja të tjera të anashkalimit të autentifikimit.
b) Shikon për sjellje jo të zakontë nga përdoruesit e autentifikuar si:
   i. autentifikime të shpeshta;
   ii. autentifikim jashtë orarit të punës;
   iii. përdorimi i shërbimeve ku përdoruesi nuk është i autorizuar.
c) Kërkon në sistem për prezencën e skedarëve si **.exe**, **.vbs**, **.ps1** (*windows*) , **.py, .sh** (*linux*) kryesisht në direktorinë **tmp.**
ç) Kërkon për tasket e programuara: task scheduler (*windows*) dhe komandat **crontab -l**, **ls /etc/cron.*** në *Linux.*
d) Monitoron për llogari të krijuara në sistem duke përdorur komanda si: lusrmgr.msc (Windows) dhe komanden cat /etc/passwd (Linux) etj. Për përdoruesit e domain, shikon pemën e përdoruesve në *Active Directory*.
dh) Raporton menjëherë sapo evidenton anashkalim të autentifikimit drejt CSIRT-it kombëtar dhe atij sektorial.
e) Ruan log-e dhe të dhënat e lidhura me anashkalimin e autentifikimit për analizime të mëtejshme.

5.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Identifikon incidentin e anashkalimit të autentifikimit përmes analizës nga të dhënat e mbledhura.
b) Identifikon shtrirjen dhe ndikimin e mundshëm të incidentit për sigurinë kombëtare dhe në të gjitha infrastrukturat kritike dhe të rëndësishme.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit rreth incidentit të identifikuar si anashkalim i autentifikimit dhe ndikimet e saj të mundshme.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit lidhur me anashkalimin e autentifikimit të raportuar nga operatorët dhe vlerëson ndikimin e saj në asetet specifike të sektorit.
b) Koordinohetn me operatorët për të përcaktuar nivelin e rrezikut që sjell anashkalimi i autentifikimit brenda sektorit.
c) Ofron informacion të detajuar të incidentit drejt CSIRT-it kombëtar për një analizë të detajuar.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton anashkalimin e autentifikimit, duke përfshirë në dokumentim metodën, origjinën dhe qëllimin e mundshëm.
b) Identifikon privilegjet e përdoruesit që është qasur në mënyrë të paautorizuar.
c) Aplikon Yara Rules për të gjetur skedarët keqdashës.
ç) Identifikon IP me të cilat sistemet komunikojnë. Mund të përdoren programe si **Wireshark**, **Task Manager => Performance => Resource monitor**, **tcpview** (Sysinternals Suite), komanda **netstat -ano** (Windows cmd), për sistemet **Linux** përdorni **netstat -tulpn** dhe **netstat -tupn**, ose **lsof -i.**
d) Përdor komandën "Get-FileHash" në PowerShell (Windows) ose “sha256sum” (Linux) për të marrë vlerën e hash SHA-256 të skedarit keqdashës të zbuluar.
dh) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial, duke dhënë të gjitha të dhënat përkatëse dhe analizën fillestare.
e) Ndihmon në identifikimin e qëllimit të anashkalimit të autentifikimit dhe ndikimin e mundshëm në shërbimet e infrastrukturës.

5.4 Komunikimi dhe Koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe atij pranë operatorit.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT Sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.

c) Kryen takime të rregullta me operatorët dhe CSIRT -et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informon në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

5.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidenteve bashkë me detajet rreth incidentit.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit në mbledhjen e informacionit të nevojshëm rreth incidentit për të arritur në dokumentimin e plotë.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në regjistrimin e incidentit në platformën e menaxhimit të incidenteve dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Mbledh dhe dërgon të dhënat mbi incidentin drejt CSIRT-it kombëtar, duke qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton hapat e ndërmarra në menaxhimin e incidentit dhe e rregjistron atë sipas përcaktimeve të rregullores së kategorizimit të incidenteve kibernetike.
b) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial.

5.6 Kategorizimi i Incidentit

CSIRT Kombëtar

a) Kategorizon anashkalimin e autentifikimit si incident bazuar në natyrën, shtrirjen dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Klasifikon incidentin sipas ashpërsisë së tij, duke marrë parasysh dëmin e mundshëm dhe sistemet e shënjestruara.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin e incidentit dhe jep udhëzime për veprimet e menaxhimit të incidenteve.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit si anashkalim autentifikimi brenda sektorit, bazuar në ndikimin dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e natyrës së anashkalimit dhe rëndësinë apo impaktin e saj në operacionet sektoriale.

CSIRT pranë operatorit

a) Kategorizon dhe raporton përpjekjet për anashkalim të autentifikimit.
b) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.
c) Zbaton masa të menjëhershme për të ndaluar dëmet e shkaktuara nga përpjekja për anashkalimin e autentifikimit.

5.7 Prioritizim i incidentit

CSIRT kombëtar

a) Vlerëson kritikalitetin e anashkalimit të autentifikimit bazuar në potencialin e saj për të kompromet uar të dhëna të ndjeshme ose për të ndërprerë shërbimet kritike.
b) Prioritizon reagimin ndaj incidentit, duke u fokusuar në ato incidente që mund të çojnë në shkelje të rëndësishme të sigurisë.
c) Koordinohet me CSIRT-et sektoriale dhe ato pranë operatorit për të siguruar që incidentet më kritike të trajtohen me prioritet.

CSIRT Sektorial

a) Vlerëson ndikimin e përpjekjeve për ndërhyrje në shërbimet kritike të sektorit dhe i prioritizon ato sipas nevojës.
b) Koordinon me CSIRT-in pranë operatorit me qëllim prioritizimin dhe sinkronizimin e përgjigjes ndaj incidentit.
c) Bashkëpunon me CSIRT-in pranë operatorëve me qëllim zbutjen e kërcënimeve më kritike të identifikuara përmes incidentit.

CSIRT pranë operatorit

a) Vlerëson ndikimin e anashkalimit të autentifikimit në proceset operacionale dhe prioritizon veprimet e reagimit sipas nevojës.
b) Siguron që çdo dëm potencial ose kompromet im i të dhënave të menaxhohet dhe adresohet menjëherë.
c) Raporton vendimet për prioritizim tek CSIRT-i kombëtar dhe ai sektorial, duke ofruar analizime dhe arsyetime.

5.8 Analiza e Incidentit

CSIRT Kombëtar

a) Kryen analizë të plotë të incidentit të cilësuar si anashkalim autentifikimi, duke u fokusuar në origjinën, metodën dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë.
c) Shpërndan analizimet me CSIRT-et sektoriale dhe ato pranë operatorëve për të ndihmuar në përgjigjet specifike për sektorin dhe përpjekjet e parandalimit në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në analizimin e anashkalimit të autentifikimit, duke shfrytëzuar informacionet e mbledhura dhe inteligjencën e kërcënimeve.

b) Asiston CSIRT-in pranë operatorit në identifikimin e dobësive të shfrytëzuara nga anashkalimi i autentifikimit dhe sugjeron strategji për reduktimin e dobësive.
c) Siguron shpërndarjen e raportit të analizës drejt CSIRT-it kombëtar për qartësim të situatës.

CSIRT pranë operatorit

a) Analizon anashkalimin e autentifikimit në nivel operativ, duke u fokusuar në mënyrën se si mund të ndikojë në sistemet kritike dhe të dhënat.
b) Shkarkon memorjen (memory dump) duke përdorur mjete si FTK ose alternative, me qëllim analizimin e thelluar nga instancat përkatëse.
c) Mban evidenca si klonimi në gjendjen aktuale të sistemit.
ç) Shpërndan gjetjet me CSIRT-in kombëtar dhe atë sektorial për të kontribuar në një kuptim më të gjerë të incidentit.
d) Përdor gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar përpjekjet e mëtejshme për anashkalim.

5.9 Izolimi dhe fshirja

CSIRT Kombëtar

a) Ofron udhëzime dhe mbështetje për reduktimin e ndikimit për anashkalimin e autentifikimit.
b) Koordinon përpjekjet me CSIRT-et sektorial dhe atë pranë operatorit për të siguruar që strategjitë e reagimit të zbatohen në të gjitha sektorët.
c) Adreson çdo dobësi të ekspozuar nga anashkalimi autentifikimit, duke siguruar reduktimin dhe parandalimin e rasteve të ngjashme në të ardhmen.

CSIRT Sektorial

a) Koordinon me CSIRT-in pranë operatorit me qëllim marrjen e masave parandaluese në të gjithë sektorin për të parandaluar shfrytëzimin e mëtejshëm të dobësive.
b) Punon ngushtë me operatorët për të siguruar reduktimin e dobësive për përpjekjet për ndërhyrje.
c) Monitoron situatën për të siguruar që të gjitha dobësitë e identifikuara janë adresuar dhe incidenti është zgjidhur plotësisht.

CSIRT pranë operatorit

a) Adreson menjëherë çdo dobësi të identifikuar nga autentifikimi.
b) Çaktivizon përdoruesit e kompromentuar.
c) Ndjek procedurat parandaluese dhe të zbutjes të ofruara nga CSIRT-i kombëtar dhe ai sektorial, duke siguruar që të gjitha hapat e nevojshëm të ndërmerren.

5.10 Rikthimi i shërbimeve / të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e çdo shërbimi të prekur si pasojë e anashkalimit të autentifikimit.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Monitoron sistemet gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidentet në të ardhmen.

CSIRT Sektorial

a) Ndihmon në rikthimin e shërbimeve sektoriale, duke prioritizuar shërbimet ose sistmet më kritike të prekura.
b) Mbështet operatorët në rikthimin e shërbimeve në kapacitetin e plotë operacional.
c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim drejt CSIRT-it kombëtar dhe palët e treta të prekura.

CSIRT pranë operatorit

a) Rikthen shërbimet e prekura nga incidenti, duke ndjekur planet e rikuperimit të hartuara. Hapat që mund të aplikohen janë:
   i. rikthimi i sistemeve përmes kopjeve rezervë (*backups*);
   ii. ndryshimi fjalëkalimeve për përdoruesit;
   iii. aplikimi i qasjes me disa faktorë (MFA).
b) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikuperuara përpara se ato të rifillojnë operacionet normale.
c) Raporton progresin e rikuperimit dhe çdo problematikë të hasur gjatë procesit të rikuperimit drejt CSIRT-it kombëtar dhe atij sektorial.
ç) Monitoron trafikun për aktivitete të dyshimta që vazhdojnë edhe pas rikthimit të shërbimit.

5.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport të plotë në lidhje me anashkalimin e autentifikimit, veprimet e reagimit ndaj incidentit dhe rezultatet.
b) Kryen rishikim pas incidentit për të identifikuar mësimet e nxjerra dhe ku ka më tepër nevojë për përmirësim.
c) Shpërndan raportet me CSIRT-in sektorial dhe atë pranë operatorit për të përmirësuar reagimin ndaj incidenteve në të ardhmen.

CSIRT Sektorial

a) Përgatit një raport për sektorin specifik mbi ndikimin e incidentit, hapat e ndërmarrë për menaxhimin e tij dhe përfundimet.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke dhënë rekomadime specifike për sektorin.
c) Shpërndan raportet dhe mësimet e nxjerra brenda sektorit për të përmirësuar reagimin ndaj incidenteve në të ardhmen.

CSIRT pranë operatorit

a) Harton një raport përfundimtar duke ofruar informacion të detajuar mbi ndikimin që incidenti ka pasur, reagimi ndaj tij dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësime operacionale dhe duke përditësuar planet e reagimit.
c) Nxjerr përfundimet për ndryshimet që duhen aplikuar për të rritur nivelin e sigurisë për të shmangur incidentet në të ardhmen si:

   i. Segmentimi i rrjetit

ii. Konfigurimi i firewall
iii. Siguria e aplikacionit
iv. Procedura për përditësimin e sistemeve apo aplikacioneve

ç) Zbaton rekomandimet për të forcuar mbrojtjen dhe për të përmirësuar zbulimin për sulmet e ardhshme siç janë autentifikim i paautorizuar.

6) Sulmet Vëllimore

Karakteristikat kryesore të një sulmi DDoS janë:

Shpërndarja: Aktorët keqdashës përdorin një rrjet të kompromentuar të pajisjeve, të cilat janë të infektuara me *malware* ose *botnet* për të dërguar trafik të madh të njëherëshëm në një shërbim specifik ose në një rrjet. Ky trafik është i shpërndarë në mënyrë që të bëhet e vështirë për t'u ndaluar.

Objektivi është të mos lejojë që shërbimi ose rrjeti të përdoret normalisht. Kjo ndërprerje e shërbimit ka për qëllim dëmtimin e operacioneve të infrastrukturës, impakt në reputacion, dëmtimin e integritetit të të dhënave apo shpërqëndrimin nga sulme të tjera që mund të ndodhin paralelisht.

6.1 Përgatitja

CSIRT Kombëtar

a) Harton dhe mirëmban politika dhe procedura specifike për zbulimin dhe reagimin ndaj sulmeve vëllimore, të quajtur ndryshe sulmet DDoS (distributed denial-of-service).
b) Zbaton dhe përditëson rregullisht zgjidhjet për mbrojtjen ndaj DDoS, si filtrimi i trafikut dhe sistemet për kufizimin e shpejtësisë në të gjithë rrjetet kombëtare.
c) Kryen trajnime të rregullta për analistët e CSIRT-it kombëtar mbi njohjen dhe reagimin ndaj skenarëve të sulmeve vëllimore.
d) Bashkëpunon me organet përgjegjëse me qëllim ndërlidhjen me ofruesit e shërbimeve të internetit (ISP) dhe ofruesit e shërbimeve cloud për të mundësuar një reagim të shpejtë ndaj sulmeve vëllimore.
dh) Cakton personat përgjegjës që do ndjekin incidentin dhe përcakton rolet dhe përgjegjësitë e tyre për t'u përgjigjur ndaj sulmit.

CSIRT Sektorial

a) Asiston operatorët e infrastrukturave nëpërmjet udhëzimeve për sektorin specifik për mbrojtjen kundër sulmeve vëllimore, duke siguruar përputhjen me strategjitë kombëtare.
b) Asiston operatorët e infrastrukturave në implementimin e mjeteve për shmangien e sulmeve vëllimore në pikat hyrëse dhe segmentet kritike të rrjetit.
c) Kryen trajnime për ekipet e CSIRT-it sektorial dhe atë pranë operatorit mbi zbulimin dhe zbutjen e sulmeve vëllimore, duke përfshirë identifikimin e ngjarjeve me rrezik të lartë.
ç) Bashkëpunon me CSIRT-in pranë operatorit me qëllim kryerjen vazhdimisht të testeve për rrjetin e sektorit përkatës për të vlerësuar qëndrueshmërinë kibernetike ndaj sulmeve vëllimore.

CSIRT pranë operatorit

a) Implementon masa mbrojtëse kundër sulmeve vëllimore, duke përfshirë filtrimin e trafikut dhe kufizimin e shpejtësisë.

b) Trajnon stafin për kuptuar shenjat e sulmeve vëllimore dhe raportimin e tyre menjëherë.
c) Aplikon teknikën e balancimit të ngarkesës (*load balance*) për ta shpërndarë volumin e trafikut dhe për të ulur ndikimin e sulmit.
ç) Përditëson rregullisht konfigurimet e firewall dhe aplikon rregulla në sistemet e mbrojtjes IDS/IPS rreth kërcënimeve më të fundit në lidhje me sulmet vëllimore.

6.2 Zbulimi

CSIRT Kombëtar

a) Monitoron vazhdimisht rrjetet kombëtare për shenja të sulmeve vëllimore, si rritje të papritura të trafikut të rrjetit.
b) Përdor burime të inteligjencës për kërcënimet dhe mjete të zbulimit të anomalive për të identifikuar aktivitete të mundshme të sulmeve vëllimore.
c) Bashkëpunon me CSIRT-in sektorial dhe atë pranë operatorit për të ndarë të dhënat e zbulimit dhe për të përmirësuar ndërgjegjësimin e përgjithshëm për situatën.

CSIRT Sektorial

a) Bashkëpunon me CSIRT-in pranë operatorit me qëllim implementimin e mjeteve specifike për të zbuluar sulmet vëllimore që synojnë infrastrukturën kritike.
b) Asiston operatorët për përdorimin e mjeteve shtesë ose ndryshimin e konfigurimeve për zbulimin më të mirë të sulmeve nëse rriten nivelet e kërcënimit.
c) Ndan tentativat e zbuluara për sulme vëllimore me CSIRT-in kombëtar dhe CSIRT-et e tjera sektoriale me qëllim koordinimin kundër reagimit ndaj incidentit.

CSIRT pranë operatorit

a) Përdor mjetet e monitorimit të rrjetit për të zbuluar rritje ose vlera anormale të trafikut që mund të sinjalizojnë një sulm vëllimor (DDoS).
b) Konfiguron sisteme automatike që njoftojnë në rastet kur nivelet e trafikut tejkalojnë limitet e paracaktuara.
c) Raporton menjëherë çdo përpjekje të zbuluar për sulm vëllimor drejt CSIRT-it kombëtar dhe atij sektorial.
ç) Ruan loge dhe të dhënat e lidhura me sulmet vëllimore të zbuluara për analiza dhe përgjigje të mëtejshme.

6.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Konfirmon prezencën e sulmit vëllimor përmes analizës së thelluar, duke shfrytëzuar burimet kombëtare të inteligjencës.
b) Koordinohet me CSIRT-et sektoriale për të sinkronizuar të dhënat e identifikimit dhe për të krijuar një pasqyrë të plotë të sulmit në shkallë kombëtare.
c) Njofton CSIRT-et përkatëse sektoriale dhe ato pranë operatorëve rreth sulmit vëllimor të identifikuar dhe ndikimeve të mundshme.

CSIRT Sektorial

a) Koordinohet me operatorët lidhur me sulmin vëllimor të raportuar nga vetë ata dhe vlerëson ndikimin e tij në asetet të sektorit.
b) Koordinohet me operatorët për të përcaktuar shkallën e sulmit vëllimor brenda sektorit.

c) Jep informacion të detajuar të incidentit drejt CSIRT-it kombëtar për një analizë të plotë.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton sulmin vëllimor, duke përfshirë burimin, metodën dhe objektivat e mundshme bazuar në analizën e trafikut dhe log-e.
b) Identifikon sistemet e prekura, dhe shtrirjen e sulmit në sisteme tjera, nëse ka.
c) Raporton incidentin tek CSIRT-i kombëtar dhe ai sektorial, duke ofruar të gjitha të dhënat përkatëse dhe analizën fillestare.
ç) Identifikon qëllimin e sulmit dhe ndikimin e tij të mundshëm në shërbime operacionale.

6.4 Komunikimi dhe Koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit.
b) Komunikon me organet kompetente në vend për bllokimin në shkallë kombëtare të IP-ve të cilësuara si keqdashëse pas analizimeve të kryera.
c) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
ç) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT Sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

6.5 Regjistrimi

CSIRT kombëtar

a) Regjistron si incident sulmin vëllimor në sistemin kombëtar të menaxhimit të incidenteve, duke siguruar që të gjitha të dhënat e mbledhura të jenë të regjistruara.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të mbledhur informacion shtesë dhe për të siguruar që incidenti të jetë dokumentuar plotësisht.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur nga incidenti me qëllim regjistrimin e sulmit vëllimor në platformën e menaxhimit të incidenteve, bazuar në dokumentacion.
b) Koordinon me CSIRT-in pranë operatorit me qëllim që të gjithë operatorët e prekur të jenë të përfshirë në procesin e regjistrimit.
c) Dërgon informacionet dhe detajet e incidentit të mbledhura tek CSIRT-i kombëtar për të qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton sulmin vëllimor dhe çdo gjetje fillestare bazuar në të dhënat e mbledhura.
b) Siguron regjistrimin e duhur në sistemin e menaxhimit të incidenteve sipas përcaktimeve në rregulloren për kategorizimin e incidenteve kibernetike.
c) Raporton incidentin tek CSIRT-i kombëtar dhe ai sektorial me të gjitha detajet përkatëse.

6.6 Kategorizimi i Incidentit

CSIRT Kombëtar

a) Kategorizon si incident kibernetik përmes analizës së të dhënave të trafikut të rrjetit dhe treguesve të tjerë sulmin vëllimor.
b) Kategorizon sulmin vëllimor bazuar në natyrën, shtrirjen dhe ndikimin e mundshëm në sigurinë kombëtare.
c) Klasifikon incidentin sipas ashpërsisë së tij, duke marrë parasysh ndërprerjen e mundshme të shërbimeve kritike.
ç) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin dhe ofron udhëzime për veprimet e duhura të përgjigjes.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e sulmit vëllimor brenda sektorit, bazuar në ndikimin dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e natyrës specifike të sulmit vëllimor dhe rëndësinë e tij për operacionet sektoriale.

CSIRT pranë operatorit

a) Kategorizon dhe raporton sulmin vëllimor, duke siguruar që të gjitha informacionet ndihmojnë në kategorizimin e incidentit.
b) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.
c) Zbaton masa të menjëhershme për të zbutur çdo dëm të shkaktuar nga sulmi vëllimor.

6.7 Prioritizim i incidentit

CSIRT Kombëtar

a) Vlerëson rëndësinë e sulmit vëllimor bazuar në potencialin e tij për të ndërprerë shërbimet kritike ose për të kompromentuar sigurinë kombëtare.
b) Prioritizon përgjigjen ndaj incidentit, duke u fokusuar në ato incidente që mund të çojnë në ndërprerje të rëndësishme.
c) Koordinon me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që incidentet më kritike të trajtohen me shpejtësi.

CSIRT Sektorial

a) Vlerëson ndikimin e sulmit vëllimor në shërbimet kritike të sektorit dhe asiston CSIRT-in pranë operatorit me qëllim prioritizimin sipas nevojës dhe koordinimin e reagimit ndaj sulmit.
b) Koordinohet me CSIRT -in pranë operatorit me qëllim evitimin e kërcënimeve me nivel rreziku më të lartë të identifikuara përmes sulmit vëllimor.

CSIRT pranë operatorit

a) Vlerëson ndikimin e sulmit vëllimor në proceset operacionale dhe prioritizon veprimet e përgjigjes ndaj sulmit sipas nevojës.
b) Siguron që çdo ndërprerje e mundshme e shërbimeve të jetë menaxhuar dhe adresuar menjëherë.
c) Raporton vendimet për prioritizim drejt CSIRT-it sektorial dhe atij kombëtar, bazuar në analizime dhe arsyetime.

6.8 Analiza e Incidentit

CSIRT Kombëtar

a) Kryen një analizë të plotë të sulmit vëllimor, duke u fokusuar në origjinën e sulmit, metodën dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë.
c) Shpërndan rezultatet e analizës me CSIRT-et sektoriale dhe ato pranë operatorëve për të ndihmuar në reagimin më të shpejtë ndaj incidentit dhe parandalimit të sulmeve të ngjashme në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në analizimin e sulmit për sektorin e prekur, duke shfrytëzuar informacionet e mbledhura dhe inteligjencën e kërcënimeve.
b) Asiston CSIRT-in pranë operatorit në identifikimin e dobësive të shfrytëzuara nga sulmi dhe sugjeron strategji të zbutjes.
c) Vendos në dispozicion të CSIRT-it kombëtar dhe atij pranë operatorit të dhënat e analizës që shërbejnë për të kuptuar situatën dhe shtrirjen e sulmit.

CSIRT pranë operatorit

a) Analizon sulmin vëllimor në nivel operativ, duke u fokusuar në ndikimin e tij mbi sistemet dhe shërbimet kritike, përfshirë degradimin e performancës ose ndërprerje të pjesshme.
b) Analizon natyrën e sulmit për të përcaktuar nëse qëllimi kryesor i tij është shpërqendrimi nga një sulm tjetër më i sofistikuar apo ndërprerja e drejtpërdrejtë e shërbimeve operacionale.
c) Mbledh dhe analizon log-e për evidentimin e IP-ve keqdashëse, dhe i cilëson këto IP si indikatorë të kompromentimit (IOC).
ç) Analizon portat dhe shërbimet e synuara nga aktorët keqdashës për të identifikuar dobësitë e mundshme dhe objektivat kryesore të sulmit vëllimor.
d) Shpërndan gjetjet me CSIRT-et për të kontribuar në një kuptim më të gjerë të sulmit.

dh) Implementon gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar sulme të mëtejshme vëllimore.

6.9 Izolimi dhe fshirja

CSIRT kombëtar

a) Ofron udhëzime dhe mbështetje për zbutjen e ndikimit të sulmeve vëllimore të identifikuara.
b) Koordinon përpjekjet me CSIRT-et sektoriale dhe ato pranë operatorit për të siguruar që të zbatohen strategjitë nga të gjithë sektorët.
c) Drejton përpjekjet për të adresuar çdo dobësi të ekspozuar nga sulmi vëllimor, duke siguruar reduktimin dhe parandalimin e rasteve të ngjashme në të ardhmen.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit me qëllim marrjen e masave mbrojtëse për të parandaluar ndërprerje të mëtejshme nga sulmi vëllimor.
b) Punon ngushtë me operatorët për të siguruar zbutjen efektive të ndikimit të sulmit vëllimor.
c) Monitoron situatën për të siguruar që të gjitha dobësitë e identifikuara janë adresuar dhe incidenti është zgjidhur plotësisht.

CSIRT pranë operatorit

a) Adreson menjëherë çdo dobësi të identifikuar përmes sulmit vëllimor.
b) Ndjek procedurat e zbutjes të ofruara nga CSIRT-i kombëtar dhe ai sektorial, duke siguruar që të gjitha hapat e nevojshëm janë ndërmarr. Në varësi të shërbimeve të prekura sugjerohen masat e mëposhtme:

i. Rastet kur paketat shfrytëzojnë portat **TCP** kemi të bëjm me **SYN** Flood.
   a. Konfiguro Firewall, IDS dhe IPS duke filtruar trafikun nga IP që nisin trafik në masë.
ii. Rastet kur paketat shfrytëzojnë portat **UDP** kemi të bëjmë me **UDP** Flood.
   a. Limitoni numrin e paketave UDP në ardhje;
iii. **DNS Reflection** (Shfrytëzon open DNS resolver për ta ngarkuar serverin gjatë procesit të DNS response).
   a. Raste të tilla shfrytëzohen për të gjeneruar trafik me Bandwith të lartë, ku si zgjidhje në këtë rast është kontakti me **ISP**, për të kaluar IP tonë në DDoS protection.
   b. Në rast se sulmi DDoS po shfrytëzon një dobësi të sistemit për të krijuar DDoS attack pa gjeneruar bandwith të lartë, duhet konfiguruar **DNS filter**.
iv. **NTP** shfrytëzon open NTP servers.
   a. Nëse versioni NTP është më i vogël se 4.2.7, rekomandohet upgrade 4.2.7+
      i. Nëse nuk është i mundur upgrade, rekomandohet të bëhet **disable monlist dhe implementimi Ingress Filtering.**
   b. Përdorni NTP filtering.
v. **SSDP** shfrytëzon UPnP (Universal Plug and Play) për të shkaktuar DDoS
   a. Bllokimi i trafikut në portën 1900.
vi. **XML-RPC** shfrytëzon kërkesat XML-RPC të cilat përmbajnë strukturë të dhënash dhe informacion të ngarkuar duke konsumuar resurset e serverit.

a. Implementimi i *Rate-Limiting* dhe request filtering për kërkesat XML
b. Përdorni IP Whitelist ose Blacklist për ato IP që doni të lejoni ose jo.

vii. **Rekomandime të tjera:**

viii. Nëse po shihni shumë trafik në mbërritje (incoming requests) në **webserver logs**, ose **bandwidth të mbushur**, kjo mund të tregojë nje sulm i cili po përpiqet të bllokojë shërbimin tuaj në internet. Veçoni asetet tuaja kritike, identifikoni shërbimet të cilat janë të ekspozuar në internet dhe dobësitë e këtyre shërbimeve.

c) Verifikon efektivitetin e përpjekjeve për përmbajtje dhe zbutje dhe raporton statusin tek CSIRT-i kombëtar.

6.10 Rikthimi i shërbimeve / të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e shërbimeve apo sistemeve të prekura nga sulmi vëllimor në operacione normale.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Asiston CSIRT-in pranë operatorit në monitorimin e sistemeve gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidente të ardhshme.

CSIRT Sektorial

a) Ndihmon në rikuperimin e shërbimeve specifike sektoriale, duke prioritizuar shërbimet dhe sistemet më kritike të prekura.
b) Mbështet operatorët në rikthimin e shërbimeve në kapacitetin e plotë operacional.
c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim tek CSIRT-i kombëtar dhe palët e treta të përfshira në incident.

CSIRT pranë operatorit

a) Rikuperon shërbimet e prekura nga sulmi vëllimor, duke ndjekur planet e rikuperimit të vendosura.
b) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikuperuara para se të rifillojnë operacionet normale.
c) Dokumenton dhe raporton progresin e rikuperimit dhe çdo problematikë drejt CSIRT-it kombëtar dhe atij sektorial për ndihmë të mëtejshme.

6.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport të detajuar mbi sulmin vëllimor, veprimet e përgjigjes ndaj incidentit dhe rezultatet.
b) Kryen rishikim pas incidentit për të identifikuar mësimet e nxjerra dhe për të rritur aftësitë e zbulimit dhe reagimit ndaj sulmeve.
c) Shpërndan raportin me CSIRT-in sektorial dhe atë pranë operatorit për të rritur gatishmërinë e përgjithshme.

CSIRT Sektorial

a) Përgatit një raport për sektorin që përshkruan ndikimin e sulmit vëllimor, veprimet e reagimit ndaj incidentit dhe përpjekjet e rikuperimit.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke kontribuar me njohuri dhe rekomandime specifike për sektorin.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar aftësitë e zbulimit dhe përgjigjes në të ardhmen.

CSIRT pranë operatorit

a) Harton një raport përfundimtar duke ofruar informacion të detajuar mbi ndikimin e sulmit vëllimor, përgjigjen dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësime operacionale dhe duke përditësuar planet e përgjigjes.
c) Zbaton rekomandimet për të forcuar mbrojtjen dhe për të përmirësuar zbulimin e ardhshëm të sulmeve vëllimore.

7) Siguria e përmbajtjes së informacionit

Siguria e Përmbajtjes së Informacionit përfshin masat dhe praktikat e implementuara për të mbrojtur konfidencialitetin, integritetin dhe disponueshmërinë e informacionit dhe të dhënave brenda një organizate. Kjo përfshin një spektër të gjerë strategjish, teknologjish, politikash dhe procedurash të dizajnuara për të mbrojtur informacionin sensitiv nga aksesi i paautorizuar, shpërndarja e paautorizuar, ndryshimi dhe shkatërrimi. Në rastet kur kemi të bëjmë me thyerje të autorizimit në aksesimin, apo modifikimin e informacionit ndiqen hapat si më poshtë:

7.1 Përgatitja

CSIRT Kombëtar

a) Harton dhe mirëmban politika dhe procedura specifike për zbulimin dhe reagimin ndaj incidenteve të sigurisë së përmbajtjes së informacionit.
b) Zbaton dhe përditëson rregullisht zgjidhjet teknologjike për sigurinë e përmbajtjes së informacionit, si filtrimi i të dhënave dhe klasifikimi i informacionit.
c) Kryen trajnime të rregullta për analistët e CSIRT-it kombëtar mbi praktikat më të mira për mbrojtjen e përmbajtjes së informacionit dhe përgjigjen ndaj incidenteve.
ç) Bashkëpunon me CSIRT-in sektorial dhe atë pranë operatorit për të mundësuar një reagim të shpejtë dhe të koordinuar ndaj incidenteve të sigurisë së informacionit.
d) Cakton personat përgjegjës që do ndjekin incidentin dhe përcakton rolet dhe përgjegjësitë e tyre.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit nëpërmjet udhëzimeve specifike për sektorët për mbrojtjen e përmbajtjes së informacionit, duke siguruar përputhjen me politikat kombëtare.
b) Asiston CSIRT-in pranë operatorit lidhur me implementimin e mjeteve për mbrojtjen e përmbajtjes së informacionit në pikat hyrëse të rrjetit dhe sistemet kritike të sektorit.

c) Kryen trajnime për ekipet e CSIRT-it sektorial dhe atij pranë operatorit për identifikimin dhe përgjigjen ndaj incidenteve që prekin sigurinë e përmbajtjes së informacionit.
ç) Asiston CSIRT-in pranë operatorit në kryerjen e testimeve të rregullta të sistemit për të vlerësuar qëndrueshmërinë kibernetike ndaj incidenteve të përmbajtjes së informacionit.

CSIRT pranë operatorit

a) Implementon masa mbrojtëse për përmbajtjen e informacionit, duke përfshirë kriptimin, kontrollin e aksesit dhe teknikat e klasifikimit të të dhënave.
b) Trajnon stafin për të identifikuar shenjat e incidenteve të sigurisë së përmbajtjes së informacionit dhe për t'i raportuar ato menjëherë.
c) Përditëson rregullisht konfigurimet e sigurisë dhe aplikon rregulla në sistemet e mbrojtjes IDS/IPS në lidhje me kërcënimet më të fundit për përmbajtjen e informacionit.
ç) Zbaton teknika të menaxhimit të informacionit për të parandaluar aksesin e paautorizuar dhe për të mbrojtur të dhënat kritike.

7.2 Zbulimi

CSIRT Kombëtar

a) Monitoron vazhdimisht rrjetin kombëtar për shenja të incidenteve të sigurisë së përmbajtjes së informacionit, si akses të paautorizuar ose ndryshime të papritura në të dhëna.
b) Përdor burime të inteligjencës për kërcënimet dhe mjete të zbulimit të anomalive për të identifikuar aktivitete të mundshme që prekin përmbajtjen e informacionit.
c) Bashkëpunon me CSIRT-in sektorial dhe atë pranë operatorit për të ndarë të dhënat e zbulimit dhe për të përmirësuar aftësinë për reagim ndaj situatës.

CSIRT Sektorial

a) Bashkëpunon me CSIRT-in pranë operatorit mbi implementimin e mjeteve specifike për të zbuluar incidentet që synojnë përmbajtjen kritike të informacionit.
b) Asiston CSIRT-in pranë operatorit për përdorimin e mjeteve shtesë ose ndryshimin e konfigurimeve për të zbuluar më mirë kërcënimet ndaj përmbajtjes së informacionit.
c) Shpërndan gjetjet rreth incidentit të sigurisë së përmbajtjes së informacionit me CSIRT-in kombëtar dhe operatorët e prekur për të koordinuar reagimin ndaj incidentit.

CSIRT pranë operatorit

a) Përdor mjetet e monitorimit për të zbuluar aktivitete të dyshimta që mund të sinjalizojnë një incident të sigurisë së përmbajtjes së informacionit.
b) Konfiguron sisteme automatike që njoftojnë në rastet kur informacioni aksesohet nga persona të paautorizuar.
c) Raporton menjëherë çdo përpjekje të zbuluar për incident të sigurisë së përmbajtjes drejt CSIRT-it kombëtar dhe atij sektorial.

7.3 Identifikimi i Incidentit

CSIRT Kombëtar

a) Konfirmon incidentin e sigurisë së përmbajtjes përmes analizës së log-eve, të dhënave të sistemit dhe treguesve të tjerë.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të sinkronizuar të dhënat e identifikimit dhe për të krijuar një pasqyrë të plotë të incidentit në shkallë kombëtare.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit rreth incidentit të identifikuar dhe ndikimeve të mundshme.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit me qëllim verifikimin e incidentit të raportuar nga vetë ata dhe vlerëson ndikimin e tij në asetet e sektorit.
b) Koordinohet me operatorët për të përcaktuar shkallën e incidentit brenda sektorit.
c) Jep informacion të detajuar të incidentit drejt CSIRT-it kombëtar për një analizë më të thelluar.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton incidentin, duke përfshirë burimin, metodën dhe objektivat e mundshme bazuar në analizën e log-eve dhe aktivitetit në sistem.
b) Identifikon skedarët e aksesuar, modifikuar apo fshirë në mënyrë të paautorizuar.
c) Identifikon indikatorët e kompromentimi si: IP, domain, hash, email etj.
ç) Identifikon sistemet e prekura dhe raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial, duke ofruar të gjitha të dhënat përkatëse dhe gjetjet fillestare si : koha kur është evidentuar incidenti, dhe sa sisteme janë prekur.
d) Mban evidenca për analizime të mëtejshme. Krijon kopje të sistemeve të prekura, duke e mbajtur për analizime më të thelluara.

7.4 Komunikimi dhe Koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikimi midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit për të siguruar një reagim të unifikuar.
b) Komunikon me autoritetet kompetente për bashkëpunim në zgjidhjen e incidenteve që prekin përmbajtjen e informacionit në nivel kombëtar.
c) Ofron përditësime të vazhdueshme dhe udhëzime për të gjitha palët përkatëse gjatë incidentit.

CSIRT Sektorial

a) Koordinohet drejtpërdrejt me CSIRT-in pranë operatorëve për të siguruar që informacionet rreth incidentit të shpërndahen në kohë për të optimizuar përgjigjen.
b) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të koordinuar veprimet dhe strategjitë e mbrojtjes.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informon në kohë reale CSIRT-in sektorial dhe atë kombëtar për çdo zhvillim të rëndësishëm dhe ndan log-et e përditësuara për analizë.

7.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron incidentin në sistemin kombëtar të menaxhimit të incidenteve, duke siguruar që të gjitha të dhënat e mbledhura të jenë të ruajtura.
b) Koordinon me CSIRT-in sektorial dhe atë pranë operatorit për të mbledhur informacione shtesë dhe për të siguruar që incidenti të jetë dokumentuar plotësisht.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur nga incidenti me qëllim regjistrimin e incidentit në platformën e menaxhimit të mundësuar nga CSIRT-i kombëtar dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Dërgon të dhëna mbi incidentin drejt CSIRT-it kombëtar për të qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton incidentin dhe çdo gjetje fillestare bazuar në të dhënat e mbledhura.
b) Siguron regjistrimin e incidentit në sistemin e menaxhimit të incidenteve sipas përcaktimeve në rregulloren e kategorizimit të incidentit të sigurisë kibernetike.
c) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial dhe me të gjitha detajet përkatëse (*log-e*).

7.6 Kategorizimi i Incidentit

CSIRT Kombëtar

a) Kategorizon incidentin e sigurisë së përmbajtjes së informacionit bazuar në natyrën, shtrirjen dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Klasifikon incidentin sipas ashpërsisë së tij, duke marrë parasysh ndërprerjen e mundshme të shërbimeve kritike, humbjen e informacionit të ndjeshëm dhe dëmtimin e reputacionit kombëtar.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin dhe ofron udhëzime për veprimet e duhura të përgjigjes.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit të sigurisë së përmbajtjes brenda sektorit, bazuar në ndikimin dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e natyrës specifike të incidentit dhe rëndësinë e tij për operacionet sektoriale.

CSIRT pranë operatorit

a) Kategorizon dhe raporton incidentin, duke siguruar që të gjitha informacionet çojnë në kategorizimin e incidentit bazuar në ndikimin në sistem dhe përmbajtjen e informacionit.
b) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij, duke përfshirë masa të menjëhershme për të siguruar informacionin.
c) Zbaton masa të menjëhershme për të zbutur çdo dëm të shkaktuar nga incidenti dhe për të parandaluar përhapjen e tij.

7.7 Prioritizimi i Incidentit

CSIRT Kombëtar

a) Vlerëson rëndësinë e incidentit të sigurisë së përmbajtjes së informacionit bazuar në potencialin e tij për të ndërprerë shërbimet kritike, për të kompromentuar të dhëna të ndjeshme dhe për të ndikuar sigurinë kombëtare.
b) Prioritizon përgjigjen ndaj incidentit, duke u fokusuar në ato incidente që mund të çojnë në dëmtim të rëndësishëm të përmbajtjes së informacionit ose të sigurisë kombëtare.
c) Koordinon me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që incidentet më kritike të trajtohen me shpejtësi dhe të ulet ndikimi i tyre.

CSIRT Sektorial

a) Vlerëson ndikimin e incidentit të sigurisë së përmbajtjes së informacionit në shërbimet kritike të sektorit dhe bën prioritizimin sipas nevojës.
b) Koordinon me CSIRT-in pranë operatorit prioritizimin duke siguruar që ata të marrin masa të menjëhershme për të zbutur ndikimin e incidentit në operacionet e tyre.
c) Asiston CSIRT-in pranë operatorit me qëllim shmangien e kërcënimeve me nivel rreziku të lartë që ndikojnë në përmbajtjen kritike të informacionit të sektorit.

CSIRT pranë operatorit

a) Vlerëson ndikimin e incidentit të sigurisë së përmbajtjes së informacionit në proceset operacionale dhe prioritizon veprimet e përgjigjes sipas rrezikshmërisë së tij.
b) Siguron që çdo ndërprerje e mundshme e shërbimeve të jetë menaxhuar dhe adresuar menjëherë, duke ruajtur integritetin e përmbajtjes së informacionit.
c) Raporton vendimet për prioritizim drejt CSIRT-it kombëtar dhe atij sektorial, bazuar në analizime dhe arsyetime të sakta.

7.8 Analiza e Incidentit

CSIRT Kombëtar

a) Kryen analizë të plotë të incidentit, duke u fokusuar në burimin e tij, metodën dhe ndikimin në sigurinë kombëtare të informacionit.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë.
c) Analizon dhe shpërndan indikatorët e kompromentimit në të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit.

ç) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në reagimin më të shpejtë ndaj incidentit.

CSIRT sektorial

a) Asiston CSIRT-in pranë operatorit në kryejen e analizës për sektorin e prekur, duke shfrytëzuar informacionet e mbledhura dhe inteligjencën e kërcënimeve.
b) Asiston me CSIRT-in pranë operatorit në identifikimin e dobësive të shfrytëzuara dhe sugjeron strategji për përmirësimin e sigurisë në nivel sektori.
c) Vendos në dipozicion të CSIRT-it kombëtar dhe atij pranë operatorit detaje nga analiza e kryer me qëllim për të ofruar informacion të detajuar rreth incidentit.

CSIRT pranë operatorit

a) Analizon incidentin në nivel operativ, duke evidentuar ndikimin mbi sistemet kritike dhe përmbajtjen e informacionit.
b) Analizon nëse incidenti ka ardhur nga persona të brendshëm të infrastrukturës apo jo.
c) Analizon log-et për të gjetur pikën e hyrjes, dhe të gjithë indikatorët që ndikojnë në kompromentimin e sistemit.
ç) Mbledh dhe analizon log-et për identifikimin e burimeve keqdashëse dhe ndan rezultatet me CSIRT- et.
d) Analizon për programe keqdashëse që mund të jenë prezent në sistem duke kërkuar specifikisht në direktorinë %TEMP% në **windows** ose /tmp në **Linux**.

7.9 Izolimi dhe fshirja

CSIRT Kombëtar

a) Ofron udhëzime dhe mbështetje për izolimin dhe zbutjen e ndikimit të incidenteve të sigurisë së përmbajtjes së informacionit.
b) Koordinon përpjekjet me CSIRT-in sektorial dhe CSIRT-in pranë operatorit për të siguruar që strategjitë e qëndrueshmerisë kibernetike, të izolimit dhe fshirjes të zbatohen në të gjitha sektorët.
c) Adreson çdo dobësi të evidentuar nga incidenti, duke siguruar reduktimin dhe parandalimin e rasteve të ngjashme në të ardhmen.
ç) Bashkëpunon me operatorët e prekur për të ndaluar aksesin e paautorizuar dhe për të fshirë përmbajtjen e kompromentuar nga sistemet dhe burimet e tjera kombëtare.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në implementimin e masave mbrojtëse për të izoluar sistemet dhe rrjetet e prekura nga incidenti, duke përfshirë bllokimin e aksesit të paautorizuar në përmbajtjen e informacionit.
b) Punon ngushtë me operatorët për të siguruar zbutjen efektive të ndikimit të incidentit dhe për të fshirë përmbajtjen e rrezikshme nga sistemet (skedarë keqdashës, përmbajtja e modifikuar, kod keqdashës etj.).
c) Monitoron situatën për të siguruar që të gjitha dobësitë e identifikuara janë adresuar dhe që incidenti është izoluar dhe fshirë plotësisht.

ç) Asiston CSIRT-in pranë operatorit për të analizuar teknikën që kanë ndjekur aktorët keqdashës për të zhvilluar masa parandaluese dhe për të përditësuar politikat rreth sigurisë së përmbajtjes së informacionit.

CSIRT pranë operatorit

a) Izolon menjëherë çdo sistem të prekur nga incidenti, duke përfshirë ndërprerjen e aksesit të paautorizuar në informacionet me përmbajtje kritike.

b) Ndjek udhëzimet e dhëna nga CSIRT-i kombëtar dhe ai sektorial për izolimin dhe zbutjen e incidentit, duke siguruar që të gjitha hapat e nevojshëm të ndërmerren për të shmangur përhapjen e tij.

- Monitoron trafikun për aktivitet të dyshimtë
- Sheh nëse ka Syslog të konfiguruar?
    - Nëse po, analizohen log-et për të parë aktivitetin se kur informacionet janë aksesuar dhe emri përdoruesit i cili e ka ndryshuar këtë informcion për herë të fundit.
    - Nëse jo, me anë të komandës në **powershell**, kuptohen skedarët e modifikuar së fundmi në Path-in specifik. **Funksioni (Get-Date).AddDays(-30),** kontrollon për skedarët e modifikuar 30 ditët e fundit, **-Filter *.exe**, kontrollon për llojin e skedarit exe.

      Windows:

      Get-ChildItem -Path C:\ -Recurse -File -Force -Filter *.exe | Where-Object { $_.LastWriteTime -gt (Get-Date).AddDays(-30) -and $_.PSIsContainer -eq $false }

      Linux:

      find / -type f -name "*.sh" -mtime -30

      find / -type f -name "*.py" -mtime -30

- Rastet kur aksesimi i paautorizuar ndodh nga persona të brendshëm personi që zotëron kompjuterin/instancën, merret në pyetje për të kuptuar më tepër rreth aksesimit të informacionit.
- Analizon loget për "**Successful Login**" në **Windows Event Viewer**, për të krijuar idenë kush dhe kur është aksesuar informacioni.

    - Kur Logon Type: 2 – Logim lokal ose përmes console.
    - Kur Logon Type: 3 – Logim përmes një direktorie shared.
    - Kur Logon Type: 10 – Logim përmes RDP.

- Analizon loget nga **DLP** ose **logserveri** për të kuptuar mënyrën e shpërndarjes si psh: log-et për përdorimin e USB, CDROM ose historiku i shfletuesve web, për të kuptuar faqet e vizituara të cilat mund të kenë shërbyer si burim i shpërndarjes së infromacionit.

Event Viewer > System Logs > Filtroni Eventet, sipas EventID 2002. (USB Connect/Disconnect).

- Nëse aksesimi është bërë nga persona të brëndshëm, bëhet një mbledhje me personelin e lidhur me këtë çështje ku të merren më tepër detaje.

c) Zbaton masa për të fshirë ose ndaluar përmbajtjen e kompromentuar nga të gjitha sistemet dhe burimet, duke përdorur mjete të kriptimit, klasifikimit dhe fshirjes së sigurt të të dhënave.

ç) Verifikon efektivitetin e përpjekjeve të izolimit dhe fshirjes dhe raporton statusin tek CSIRT-i kombëtar dhe ai sektorial. Në varësi të llojit të incidentit, sugjerohen masat e mëposhtme:

i. Akses i paautorizuar në të dhëna: Zbaton kontrolle të rrepta të aksesit dhe ndryshon kredencialet e kompromentuara për të izoluar incidentin.

ii. Ndryshim i papritur i të dhënave: Rikthen të dhënat nga kopjet rezervë të sigurta dhe monitoron për të shmangur ndryshime të mëtejshme.

iii. Përmbajtje e keqinformimit: Identifikon dhe heq përmbajtjen e rrezikshme dhe bllokon burimet që përhapin informacionin kompromentues.

7.10 Rikthimi i shërbimeve/të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e informacionit të prekur.

b) Monitoron sistemet gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidente në të ardhmen.

CSIRT Sektorial

a) Ndihmon në rikuperimin e përmbajtjes së informacionit të kompromentuar dhe mbështet operatorët në rikthimin e plotë të përmbajtjes.

b) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim drejt CSIRT-it kombëtar dhe palët e treta të prekura.

CSIRT pranë operatorit

a) Rikuperon përmbajtjen e informacionit të prekur, duke ndjekur planin e rikuperimit.

b) Verifikon integritetin e informacionit të rikuperuar.

c) Dokumenton dhe raporton progresin e rikuperimit drejt CSIRT-it kombëtar dhe atij sektorial.

7.11 Aktiviteti Pas Incidentit

CSIRT kombëtar

a) Harton një raport të detajuar mbi incidentin dhe veprimet e ndërmarra.

b) Kryen rishikim pas incidentit për të identifikuar mësimet e nxjerra dhe për të përmirësuar përpjekjet për të shmangur incidente të ngjashme në të ardhmen.

c) Shpërndan raportin me CSIRT-in sektorial dhe atë pranë operatorit për të rritur gatishmërinë për përgjigjen ndaj incidenteve të tilla në të ardhmen.

CSIRT Sektorial

a) Përgatit një raport sektorial që përshkruan ndikimin dhe përpjekjet e rikuperimit.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke kontribuar me njohuri dhe rekomandime specifike për sektorin.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar përgjigjen në të ardhmen ndaj këtyre incidenteve.

CSIRT pranë operatorit

a) Harton një raport përfundimtar duke ofruar informacion të detajuar mbi ndikimin e incidentit, përgjigjen dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar hapësirat për përmirësim me qëllim përgjigjen në kohë më të shpejtë në incidentet e ardhshme.
c) Zbaton rekomandimet për të forcuar mbrojtjen dhe zbulimin e ardhshëm të incidenteve të sigurisë së përmbajtjes së informacionit.

8) Mashtrimi

Mashtrimi zakonisht i referohet çdo aktiviteti keqdashës që ka për qëllim të mashtrojë individët ose infrastrukturat për përfitime personale, financiare ose qëllime spiunazhi. Kjo përfshin sulme phishing, vjedhje identiteti, mashtrime financiare ose çdo praktikë tjetër mashtruese që përdoret për të fituar në mënyrë të paligjshme para, informacion ose asete. Aktivitetet mashtruese shpesh shfrytëzojnë dobësitë e sigurisë, manipulojnë psikologjinë njerëzore ose përdorin taktika të inxhinierisë sociale. Karakteristika kryesore e mashtrimit në këto kategori është qëllimi për të mashtruar dhe përfituar diçka me vlerë përmes mjeteve të ndryshme.

8.1 Përgatitja

CSIRT Kombëtar

a) Harton politika dhe procedura për zbulimin dhe reagimin ndaj kërcënimeve si mashtrimi kompjuterik (faqet e rreme, phishing dhe inxhinieria sociale etj).
b) Implementon sisteme të avancuara për zbulimin e kërcënimeve, duke përfshirë teknologjitë e mashtrimit kompjuterik si *honeypots, honey tokens*, sistemet *decoy* etj.
c) Trajnon analistët e CSIRT-eve për identifikimin dhe reagimin ndaj taktikave të mashtrimit kompjuterik, duke përfshirë të kuptuarit e *false-positives*.
ç) Bashkëpunon me organizata ndërkombëtare të sigurisë kibernetike për të qëndruar të informuar mbi teknikat e reja të mashtrimit kompjuterik.
d) Përcakton personat përgjegjës për reagimin ndaj incidentit dhe rolet dhe përgjegjësitë e gjithësecilit.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit nëpërmjet udhëzimeve specifike për sektorin për identifikimin dhe zbutjen e sulmeve si mashtrimi kompjuterik, duke siguruar përputhje me strategjitë kombëtare.

b) Asiston CSIRT-in pranë operatorit në implementimin e teknologjive që ndihmojnë në zbulimin e mashtrimit kompjuterik të përshtatura për sektorin. Të tilla teknologji përfshijnë të dhëna të rreme, kredenciale, shërbime të rreme etj. që tërheqin dhe identifikojnë aktorët keqdashës.
c) Kryen trajnime të herë pas herëshme për ekipet e CSIRT-it sektorial dhe atë pranë operatorit mbi skenarët e mashtrimit kompjuterik duke e përshtatur specifikisht për nevojat e tyre.
ç) Monitoron dhe asiston CSIRT-in pranë operatorit në mënyrë të vazhdueshme dhe kujdeset që përditësimet të aplikohen rregullisht në ato sisteme ku gjejnë zbatim, me qëllim rritjen e nivelit të mbrojtjes nga sulmet që cilësohen si mashtrime kompjuterike.

CSIRT pranë operatorit

a) Implementon dhe mirëmban teknologjitë për shmangien e mashtrimit kompjuterik, duke ngritur sisteme të rreme, dhe duke krijuar të dhënat e rreme brenda mjedisit operativ.
b) Trajnon stafin për të kuptuar mashtrimin kompjuterik dhe rëndësinë e raportimit të aktiviteteve të dyshimta.
c) Përditëson rregullisht konfigurimet e sigurisë për të siguruar që ato të mbeten efektive kundër kërcënimeve të reja.

8.2 Zbulimi

CSIRT Kombëtar

a) Monitoron vazhdimisht rrjetet kombëtare për aktivitete të mashtrimit kompjuterik, si ndërveprimet me honeypots ose qasje të papritura në sistemet mashtruese (*honeypots*).
b) Përdor mjete të avancuara inteligjente për evidentimin e kërcënimeve dhe anomalive për të identifikuar sulmet e mundshme të mashtrimit kompjuterik.
c) Bashkëpunon me CSIRT-et sektoriale dhe CSIRT-in pranë operatorit për të rritur kapacitetet e zbulimit duke ndarë të dhëna mbi aktivitetet e zbuluara të mashtrimit kompjuterik.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në implementimin e mjeteve specifike që i përgjigjen sektorit për të zbuluar ndërveprimet me asetet e mashtrimit kompjuterik, si "të dhënat e rreme" (*honeypots*) etj.
b) Asiston CSIRT-in pranë operatorit nëpërmjet këshillave dhe politikave për të shmangur aksesin e paautorizuar dhe format e mashtrimit si:
   i. Imitimi i stafit nga aktorët keqdashës përmes email-it;
   ii. USB të infektuara;
   iii. Përgjimi etj.
c) Shpërndan aktivitetet e zbuluara të mashtrimit kompjuterik me CSIRT-in kombëtar dhe CSIRT-et e tjera sektoriale për të mundësuar një reagim të koordinuar.
ç) Asiston CSIRT-in pranë operatorit në monitorimin e rrjeteve specifike të sektorit për aktivitete të dyshimta që mund të tregojnë tentativa për mashtrim kompjuterik.

CSIRT pranë operatorit

a) Përdor mjetet e monitorimit të rrjetit për të zbuluar përpjekje të paautorizuara për qasje ose ndërveprime me sistemet e mashtrimit që mund të sinjalizojnë incidentin.
b) Monitoron për aktivitete të pazakonta të përdoruesve në sisteme.

c) Raporton menjëherë çdo aktivitet të zbuluar të mashtrimit kompjuterik drejt CSIRT-it kombëtar dhe atij sektorial.
ç) Ruan loget dhe të dhënat e lidhura me aktivitetet e zbuluara për analizë të detajuar.

8.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Konfirmon aktivitetin e mashtrimit kompjuterik si një incident pasi analizës së të dhënave të mbledhura.
b) Identifikoni shtrirjen dhe ndikimin që incidenti ka në sigurinë kombëtare dhe gjitha infrastrukturat kritike dhe të rëndësishme.
c) Njofton CSIRT-et përkatëse sektoriale dhe operatorët rreth aktivitetit të identifikuar të mashtrimit kompjuterik dhe implikimeve të tij të mundshme.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit për verifikimin e aktivitetit të mashtrimit kompjuterik të raportuar nga ata dhe vlerëson ndikimin e tij në asetet specifike të sektorit.
b) Koordinohet me operatorët për të përcaktuar shkallën e aktivitetit të mashtrimit kompjuterik brenda sektorit.
c) Ofron informacion të detajuar të incidentit drejt CSIRT-it kombëtar për një analizë më të detajuar.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton aktivitetin e mashtrimit kompjuterik, duke përfshirë teknikën, burimin dhe objektivin e aktoëve keqdashës.
b) Identifikon indikatorët e kompromentimit.
c) Raporton incidentin drejt CSIRT-it kombëtar sektoriale, duke mundësuar të gjitha të dhënat përkatëse nga incidenti dhe analizën fillestare.
ç) Identifikon qëllimin e aktivitetit të mashtrimit kompjuterik dhe ndikimin e tij të mundshëm në sisteme apo shërbime.

8.4 Komunikimi dhe Koordinimi

CSIRT kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.

c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

8.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidenteve dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Koordinohet me CSIRT-et sektoriale dhe ato pranë operatorit për të mbledhur informacion shtesë dhe për të siguruar që incidenti është dokumentuar plotësisht.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur nga incidenti me qëllim regjistrimin e incidentit të mashtrimit kompjuterik në platformën e menaxhimit të incidenteve, duke siguruar një dokumentacion të plotë.
b) Koordinohet me operatorët e infrastrukturave të prekur nga incidenti me qëllim që të jenë të përfshirë në procesin e regjistrimit të incidentit.
c) Dërgon informacione dhe detaje të incidentit të mbledhura drejt CSIRT-it kombëtar për të qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton incidentin e mashtrimit kompjuterik dhe çdo gjetje fillestare bazuar në të dhënat e mbledhura.
b) Siguron regjistrimin e duhur në sistemin e menaxhimit të incidenteve sipas përcaktimeve të rregullores për kategorizimin e incidenteve kibernetike.
c) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial me të gjitha detajet përkatëse.

8.6 Kategorizimi i incidentit

CSIRT Kombëtar

a) Kategorizon aktivitetin e mashtrimit kompjuterik bazuar në natyrën, shtrirjen dhe ndikimin që incidenti ka në sigurinë kombëtare.
b) Klasifikon incidentin sipas ashpërsisë së tij, duke marrë parasysh dëmin e mundshëm dhe sistemet apo shërbimet e shënjestruara.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin dhe jep udhëzime për veprimet e duhura të përgjigjes ndaj incidentit.

CSIRT sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit të mashtrimit kompjuterik brenda sektorit, bazuar në ndikimin dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e natyrës specifike të mashtrimit kompjuterik dhe rëndësinë e tij (faqet e rreme, phishing, inxhinieria sociale etj.) bazuar në informacionet e vendosura në dispozicion nga operatorët.

CSIRT pranë operatorit

a) Kategorizon dhe raporton incidentin e mashtrimit kompjuterik, duke siguruar që të gjitha informacionet përkatëse çojnë në kategorizimin e incidentit.
b) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.
c) Zbaton masa të menjëhershme për të zbutur çdo dëm të shkaktuar nga aktiviteti i mashtrimit kompjuterik.

8.7 Prioritizim i incidentit

CSIRT Kombëtar

a) Vlerëson rëndësinë e aktivitetit të mashtrimit kompjuterik bazuar në potencialin e tij për të kompromentuar të dhëna të ndjeshme ose për të ndërprerë shërbimet kritike.
b) Prioritizon përgjigjen ndaj incidentit duke u fokusuar në ato incidente që mund të çojnë në shkelje të rëndësishme të sigurisë.
c) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që incidentet më kritike të trajtohen me përparësi.

CSIRT Sektorial

a) Vlerëson ndikimin e aktivitetit të mashtrimit kompjuterik në shërbimet kritike të sektorit dhe prioritizon ato sipas nevojës.
b) Koordinon me CSIRT-in pranë operatorit prioritizimin, duke siguruar përputhshmërinë me reagimin ndaj incidentit.
c) Asiston CSIRT-in pranë operatorit në zbutjen e menjëherëshme të kërcënimeve më të rrezikshme duke u bazuar në incidentin e cilësuar si mashtrim kompjuterik.

CSIRT pranë Operatorit

a) Vlerëson ndikimin e aktivitetit të mashtrimit kompjuterik në proceset operacionale dhe prioritizon veprimet e përgjigjes sipas nevojës.
b) Siguron që çdo dëm potencial ose kompromentim i të dhënave të jetë ruajtur, dokumentuar dhe adresuar menjëherë.
c) Raporton vendimet mbi prioritizim drejt CSIRT-it kombëtar dhe atij sektorial, duke dhënë arsyetimet e nevojshme.

8.8 Analiza e Incidentit

CSIRT Kombëtar

a) Kryen analizë të plotë të aktivitetit të mashtrimit kompjuterik, duke u fokusuar në origjinën, teknikën dhe ndikimin e mundshëm të sulmit në sigurinë kombëtare.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë.

c) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në reagimin dhe përpjekjet e parandalimit të sulmeve të ngjashme në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në analizimin e aktivitetit të mashtrimit kompjuterik, duke shfrytëzuar informacionet e mbledhura dhe inteligjencën e kërcënimeve.
b) Asiston CSIRT-in pranë operatorit në identifikimin e dobësitve të shfrytëzuara nga përpjekja për mashtrim kompjuterik dhe sugjeron strategji për zbutjen e këtyre dobësive.
c) Ofron të dhënat për analizim drejt CSIRT-it kombëtar për një kuptim të plotë të situatës.

CSIRT pranë operatorit

a) Analizon aktivitetin e mashtrimit kompjuterik në nivel operativ, duke u fokusuar në mënyrën se si mund të ndikojë në sistemet dhe shërbimet kritike.
b) Analizon aktivitetin e përdoruesve dhe teknikën e ndjekur nga aktorët keqdashës që ka sjell incidentit në lidhje me:

i. Nëse kemi të bëjmë me pagesa.
   a) Komunikon me palët e treta (bankat) me qëllim marrjen e suportit të duhur për të ndaluar ose për të rikthyer pagesën.
   b) Analizon si u arrit deri te pagesa.
ii. Email Phishing.
   a) Analizon përmes *email header* burimin e përmbajtjes së mesazhit (emailit);
   b) Analizon përmbajtjen e emailit;
   c) Analizon bashkëlidhjet;
   ç) Analizon lidhjet (*link*);
   d) Analizon DNS;
   dh) Analizon trafikut në internet;
iii. Mashtrim përmes telefonit (Vishing).
   a) Kontakton me organet kompetente (policia), për të marrë detaje rreth telefonatës së kryer
iv. Inxhinjeria sociale.
   a) Merr në pyetje personat që janë mashtruar përmes inxhinierisë sociale
v. Sulm keqdashës;
   a) Analizon burimin e sulmit (shërbimet vulnerable të shfrytëzuara) ;
   b) Kontrollon për programe keqdashëse (malware, spyware etj);
vi. Analizon informacionet e mbledhur për t'i dokumentuar më pas.
vii. Vjedhja e të drejtës së autorit.
   a) Analizon burimin nga ku këto dokumente janë marrë;
   b) Analizon kush është publikuesi i materialeve;
   c) Mbledh evidenca si *screenshot*, url, orare, video etj, që shërbejnë për dokumentim;
   ç) Kontakton organet ligj-zbatuese për masa të mëtejshme.

c) Shpërndan gjetjet me CSIRT -et për të kontribuar në një kuptim më të thellë të incidentit.
ç) Implementon gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar përpjekjet e mëtejshme për mashtrimin kompjuterik.

8.9 Izolimi dhe fshirja

CSIRT kombëtar

a) Ofron udhëzime dhe mbështetje për zbutjen e ndikimit të aktiviteteve të identifikuara si mashtrimi kompjuterik.
b) Koordinon përpjekjet me CSIRT-et sektoriale dhe ato pranë operatorëve për të siguruar që strategjitë e mbrojtjes të zbatohen në të gjitha sektorët.
c) Drejton përpjekjet për të adresuar çdo dobësi të ekspozuar nga aktiviteti i mashtrimit kompjuterik, duke siguruar reduktimin dhe parandalimin e rasteve të ngjashme në të ardhmen.

CSIRT sektorial

a) Asiston CSIRT-in pranë operatorit në implementimin e masave mbrojtëse në të gjithë sektorin për të parandaluar incidente në të ardhmen.
b) Punon ngushtë me operatorët për të ulur sa më tepër aktivitetet e mashtrimit kompjuterik.
c) Monitoron situatën për të siguruar që të gjitha dobësitë e identifikuara janë adresuar dhe incidenti është zgjidhur plotësisht.

CSIRT pranë operatorit

a) Adreson menjëherë çdo dobësi të identifikuar përmes aktivitetit të mashtrimit kompjuterik.
b) Ndjek procedurat e ofruara nga CSIRT-et (kombëtar dhe sektorial) për të frenuar dhe reduktuar aktivitetet keqdashëse, duke siguruar që të gjitha hapat e nevojshëm të ndërmerren.
c) Verifikon efektivitetin e përpjekjeve për frenim dhe zbutje të aktiviteteve keqdashëse dhe raporton statusin drejt CSIRT-eve.

8.10 Rikthimi i shërbimeve / të dhënave

CSIRT kombëtar

a) Ndihmon në rikthimin e çdo shërbimi të prekur nga aktiviteti i mashtrimit kompjuterik në operacione normale.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Monitoron sistemet gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidente të ardhshme.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit me qëllim rikuperimin e shërbimeve specifike sektoriale, duke prioritizuar shërbimet apo sistemet më kritike të prekura.
b) Ndihmon operatorët në rikthimin e shërbimeve në kapacitetin e plotë operacional.
c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim drejt CSIRT-it kombëtar dhe palët e treta.

CSIRT pranë operatorit

a) Rikuperon shërbimet e prekura nga aktiviteti i mashtrimit kompjuterik, duke ndjekur planet e rikuperimit të hartuara.

b) Verifikoni integritetin dhe funksionalitetin e shërbimeve të rikuperuara para se të rifilloj operacionet normalisht.
c) Raporton progresin e rikuperimit dhe çdo problematikë gjatë rikuperimit drejt CSIRT-it kombëtar dhe atij sektorial për ndihmë të mëtejshme.

8.11 Aktiviteti pas incidentit

CSIRT kombëtar

a) Harton një raport të plotë që detajon incidentin e mashtrimit kompjuterik, veprimet e reagimit ndaj incidentit dhe rezultatet.
b) Rishikon situatën pas incidentit për të identifikuar mësimet e nxjerra dhe fushat për përmirësim, me qëllim reagimin në kohë sa më të shkurtër kundrejt incidentit.
c) Shpërndan raportin me CSIRT-in sektorial dhe atë pranë operatorit për të rritur gadishmërinë e përgjithshme.

CSIRT Sektorial

a) Përgatit një raport mbi ndikimin e incidentit të mashtrimit kompjuterik, veprimet e reagimit ndaj incidentit dhe hapat e rikuperimit.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke kontribuar me njohuri dhe rekomandime për sektorin.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar aftësitë e zbulimit dhe reagimit ndaj incidentit në të ardhmen.

CSIRT pranë operatorit

a) Harton raportin përfundimtar duke ofruar informacion të detajuar mbi ndikimin e incidentit të mashtrimit kompjuterik, përgjigjen dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësimet dhe duke përditësuar planet e përgjigjes.
c) Zbaton rekomandimet për të forcuar mbrojtjen dhe për të përmirësuar zbulimin në sulmet e mundshme në të ardhmen rreth aktiviteteve të mashtrimit kompjuterik.

9) Dobësitë

Dobësitë i referohen pikave të dobëta që sistemet mund të kenë dhe mund të shfrytëzohen nga aktorët keqdashës, për të marrë akses të paautorizuar. Dobësitë vijnë si rezultat i programeve të pa përditësuara, keqkonfigurimet e programeve ose infrastrukturës së rrjetit, dhe rastet *0-days*, ku dobësitë janë ende të panjohura. Këto dobësi evidentohen gjithashtu edhe përmes skanimeve dhe *penetration testing.*

9.1 Përgatitja

CSIRT Kombëtar

a) Implementon mjete të qendërzuara për skanimin e vulnerabiliteteve që vlerësojnë rrjetet dhe sistemet kombëtare.
b) Trajnon vazhdimisht analistët e CSIRT-it mbi teknikat e vlerësimit të vulnerabiliteteve, përdorimin e mjeteve dhe vulnerabilitetet e reja.

c) Bashkëpunon me organizata ndërkombëtare të sigurisë kibernetike për të marrë përditësime në kohë mbi vulnerabilitetet e sapo zbuluara.
ç) Ndan vazhdimisht informacion me CSIRT-in sektorial dhe atë pranë operatorit rreth dobësive më të fundit të evidentuara në teknologji.
d) Përcakton personat që do përfshihen në reagimin ndaj incidentit, rolet dhe përgjegjësitë për adresimin e vulnerabiliteteve

CSIRT sektorial

a) Ofron udhëzime specifike për sektorin për kryerjen rregullisht të vlerësimeve të vulnerabiliteteve, duke siguruar përputhjen me strategjitë kombëtare.
b) Asiston CSIRT-in pranë operatorit në implementimin e teknologjive dhe mjeteve për vlerësimin e vulnerabiliteteve të përshtatura me nevojat specifike të sektorit.
c) Trajnon ekipet sektoriale mbi rëndësinë e vlerësimeve të vulnerabiliteteve dhe përdorimin e mjeteve të vlerësimit.
ç) Prioritizon dhe adreson vulnerabilitetet bazuar në asetet kritike të sektorit.

CSIRT pranë operatorit

a) Kryen skanime rregullisht për vlerësimin e vulnerabiliteteve brenda infrastrukturës.
b) Trajnon stafin mbi rëndësinë e menaxhimit të dobësive dhe si të reagojnë ndaj tyre.
c) Siguron që të gjitha sistemet të jenë të përditësuara dhe të *patch*-ohen rregullisht për të zbutur vulnerabilitetet e njohura.
ç) Inventarizon asetetet dhe bën vlerësimin e tyre për vulnerabilitete, duke përfshirë software, pajisjet hardware dhe pajisjet e rrjetit.

9.2 Zbulimi

CSIRT Kombëtar

a) Skanon rrjetet dhe sistemet kombëtare për vulnerabilitete duke përdorur mjete të automatizuara dhe teknika manuale.
b) Korelon të dhënat nga burime të ndryshme, duke përfshirë raportet sektoriale dhe inteligjencën e kërcënimeve, për të zbuluar dhe vlerësuar vulnerabilitetet e mundshme.
c) Monitoron për çdo vulnerabilitet të ri që mund të ndikojë në sigurinë kombëtare dhe gjitha infrastrukturat kritike dhe të rëndësishme.

CSIRT Sektorial

a) Ndan vulnerabilitetet e zbuluara me CSIRT-in kombëtar dhe CSIRT-et e tjera sektoriale për një përgjigje të koordinuar.
b) Asiston CSIRT-in pranë operatorit në monitorimin e rrjetit dhe sistemeve specifike të sektorit për vulnerabilitete të reja që mund të shfaqen për shkak të ndryshimeve në mjedis ose përditësimeve të software.

CSIRT pranë operatorit

a) Përdor mjete të automatizuara për të kryer skanime periodike të infrastrukturës për të zbuluar vulnerabilitete të mundshme në sistemet dhe aplikacionet e përdorura.
b) Monitoron rrjetin për aktivitetet të dyshimtë nga aktorët keqdashës, dhe evidenton përpjekjet për të shfrytëzuar vulnerabilitetet ekzistuese.

c) Raporton menjëherë çdo vulnerabilitet të zbuluar tek CSIRT kombëtar dhe ai sektorial për analizë të specializuar.
ç) Mban log-e dhe dokumenton të gjitha vulnerabilitetet e zbuluara, përfshirë origjinën e sulmit, llojin dhe statusin e tyre për qëllime të auditimit, pajtueshmërisë dhe referencës së ardhshme.

9.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Konfirmon vulnerabilitetet nëpërmjet analizimit të dobësive të identifikuara për të përcaktuar nivelin e rrezikut për shfrytëzim, sidomos nëse janë duke u shfrytëzuar aktivisht.
b) Vlerëson riskun bazuar në ndikimin e mundshëm të vulnerabiliteteve në sigurinë kombëtare dhe gjitha infrastrukturat kritike dhe të rëndësishme.
c) Koordinohet me partnerët ndërkombëtar të sigurisë kibernetike dhe burimet e inteligjencës për të vërtetuar nëse vulnerabiliteti i identifikuar është pjesë e një kërcënimi më të madh global.
ç) Njofton CSIRT-in përkatës sektorial dhe atë pranë operatorit për vulnerabilitetet e identifikuara dhe çdo përpjekje të mundshme për shfrytëzimin e tyre.

CSIRT sektorial

a) Koordinohet me CSIRT pranë operatorit lidhur me vulnerabilitetet e raportuara nga vetë ata dhe vlerëson ndikimin e tyre në asetet specifike të sektorit.
b) Koordinohet me operatorët për të identifikuar aktorët dhe indikatorët që shfrytëzojnë dobësitë.
c) Ofron informacion të detajuar për vulnerabilitetet tek CSIRT-i kombëtar për një analizë të plotë.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton vulnerabilitetet, duke përfshirë detajet mbi ndikimin e tyre të mundshëm dhe sistemet e prekura.
b) Raporton vulnerabilitetet e identifikuara tek CSIRT-i kombëtar dhe ai sektorial, duke ofruar të gjitha të dhënat përkatëse dhe analizën fillestare.
c) Analizon trafikun e brendshëm për të identifikuar IP që tentojnë apo shfrytëzojnë dobësitë për qëllime keqdashëse, duke i cilësuar si indikatorë të kompromentimit.
ç) Identifikon rrezikun e paraqitur nga vulnerabilitetet dhe potencialin e tyre për shfrytëzim.
d) Shpërndan indikatorët e kompromentimit me CSIRT-in kombëtar dhe atë sektorial.

9.4 Komunikimi dhe Koordinimi

CSIRT kombëtar

a) Vendos kanale komunikime midis CSIRT-in kombëtar, CSIRT-in sektorial dhe atë pranë operatorit.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT Sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

9.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron vulnerabilitetet e identifikuara në sistemin kombëtar të menaxhimit të incidenteve, duke siguruar që të gjitha të dhënat e mbledhura të jenë të regjistruara.
b) Koordinohet me CSIRT-et sektoriale dhe atë pranë operatorit për të mbledhur informacion shtesë dhe për të siguruar që vulnerabilitetet të jenë dokumentuar plotësisht.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur me qëllim regjistrimin e incidentit në platformën e menaxhimit të incidenteve të mundësuar nga CSIRT-i kombëtar.
b) Koordinohet me operatorët e infrastrukturave të prekur nga incidenti me qëllim që të jenë të përfshirë në procesin e regjistrimit.
c) Dërgon informacion dhe detaje rreth vulnerabiliteteve të evidentuara drejt CSIRT-it kombëtar për të marrë rekomandimet e nevojshme për eliminimin e dobësive.

CSIRT pranë operatorit

a) Dokumenton incidentin që shfrytëzon vulnerabilitetet e operatorit dhe çdo gjetje bazuar në zbulim dhe identifikim.
b) Regjistron incidentin në sistemin e menaxhimit të incidenteve sipas përcaktimeve në rregulloren për kategorizimin e incidenteve të sigurisë kibernetike.
c) Raporton vulnerabilitetet e shfrytëzuara drejt CSIRT-it sektorial dhe atij kombëtar me të gjitha detajet përkatëse.

9.6 Kategorizimi i Incidentit

CSIRT Kombëtar

a) Kategorizon vulnerabilitetet e identifikuara bazuar në ashpërsinë, shtrirjen dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Klasifikon vulnerabilitetet sipas probabilitetit të tyre për t'u shfrytëzuar, duke marrë në konsideratë sistemet dhe të dhënat që preken.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin dhe ofron udhëzime për eliminimin e dobësive.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e vulnerabiliteteve brenda sektorit, bazuar në ndikimin e tyre dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e natyrës specifike të vulnerabiliteteve dhe rëndësinë e tyre për operacionet sektoriale.

CSIRT pranë operatorit

a) Kategorizon dhe raporton vulnerabilitetet e shfrytëzuara, duke siguruar që të gjitha informacionet përkatëse çojnë në kategorizimin e incidentit.
b) Ndjek procedurat e vendosura për menaxhimin e vulnerabiliteteve bazuar në kategorizimin e tyre.
c) Zbaton masa të menjëhershme për të zbutur çdo rast të shfrytëzimit të vulnerabiliteteve të identifikuara.

9.7 Prioritizim i incidentit

CSIRT kombëtar

a) Vlerëson rëndësinë e vulnerabiliteteve të identifikuara bazuar në potencialin e tyre për të kompromentuar të dhëna të ndjeshme ose për të ndërprerë shërbimet kritike.
b) Prioritizon zbutjen e vulnerabiliteteve, duke u fokusuar në ato që paraqesin rrezikun më të lartë për sigurinë kombëtare.
c) Koordinohet me CSIRT-et sektoriale dhe atë pranë operatorit për të siguruar që vulnerabilitetet më kritike të adresohen me shpejtësi.

CSIRT Sektorial

a) Vlerëson ndikimin e vulnerabiliteteve të identifikuara në shërbimet kritike të sektorit dhe i prioritizon sipas nevojës.
b) Koordinon me CSIRT-in pranë operatorit prioritizimin e incidentit, duke u siguruar që të ndiqen hapat e nevojshëm për menaxhimin e incidentit.
c) I jep rëndësi adresimit të dobësive që prekin sisteme apo shërbime kritike.

CSIRT pranë operatorit

a) Vlerëson ndikimin e vulnerabiliteteve të identifikuara në proceset operacionale dhe prioritizon veprimet e zbutjes sipas nevojës.
b) Siguron që çdo vulnerabilitet me probabilitet më të lartë shfrytëzimi dhe ndikimin më të lartë të adresohet menjëherë për të parandaluar shfrytëzimin e mundshëm.

c) Raporton vendimet për prioritizim drejt CSIRT-it kombëtar dhe atë sektorial të shoqëruar me arsyetimet e nevojshme.

9.8 Analiza e Incidentit

CSIRT Kombëtar

a) Kryen analizën e plotë të vulnerabiliteteve të identifikuara, duke u fokusuar në burimin e tyre, ndikimin e mundshëm dhe çdo model që paraqet rreziqe më të gjera.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione shtesë mbi vulnerabilitetet.
c) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në reagimin në kohë më të shkurtër ndaj incidenteve dhe parandalimin e tyre në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në analizimin e vulnerabiliteteve të identifikuara ose të raportuara nga operatorët si incident kibernetik.
b) Asiston CSIRT-in pranë operatorit në analizimin e faktorëve kryesor që çuan në shfrytëzimin e vulnerabiliteteve, dhe indikatorët që lidhen me incidentin.
c) Shpërndan të dhënat e analizimit drejt CSIRT-it kombëtar.

CSIRT pranë operatorit

a) Analizon vulnerabilitetet në nivel operativ, duke u fokusuar në shkakun dhe mënyrën se si ato u shfrytëzuan.
b) Shpërndan gjetjet me CSIRT-in kombëtar dhe atë sektorial për të kontribuar në një kuptim më të gjerë të situatës.
c) Zbaton gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar vulnerabilitete të ngjashme në të ardhmen.

9.9 Izolimi dhe fshirja

CSIRT Kombëtar

a) Ofron udhëzime dhe mbështetje për zbutjen e ndikimit të vulnerabiliteteve të identifikuara.
b) Koordinon përpjekjet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që strategjitë e qëndrueshmerisë kibernetike zbatohen në të gjitha sektorët.
c) Adreson çdo vulnerabilitet që mund të shfrytëzohet, për të shmangur tentativat e shfrytëzimit të dobësive në të ardhmen.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit me qëllim zbatimin e masave mbrojtëse në të gjithë sektorin për të parandaluar shfrytëzimin e vulnerabiliteteve të identifikuara.
b) Punon ngushtë me operatorët për të siguruar zbutjen efektive të vulnerabiliteteve.
c) Monitoron situatën për të siguruar që të gjitha vulnerabilitetet e identifikuara janë adresuar dhe sistemet janë të siguruara plotësisht.

CSIRT pranë operatorit

a) Adreson menjëherë çdo vulnerabilitet të identifikuar potencialisht të shfrytëzueshëm.

b) Ndjek procedurat e zbutjes dhe mitigimit të ofruara nga CSIRT -et, duke siguruar që të gjitha hapat e nevojshëm të ndërmerren.
c) Verifikon efektivitetin e përpjekjeve për eliminimin e dhe raporton statusin tek CSIRT-i kombëtar dhe ai sektorial.

9.10 Rikthimi i shërbimeve / të dhënave

CSIRT kombëtar

a) Ndihmon në rikthimin e çdo shërbimi të prekur nga shfrytëzimi i vulnerabiliteteve të identifikuara në operacione normale.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Monitoron sistemet gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidente të ardhshme.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në rikuperimin e shërbimeve specifike sektoriale, duke prioritizuar zonat më kritike dhe të prekura.
b) Asiston CSIRT-in pranë operatorit në rikthimin e shërbimeve në kapacitetin e plotë operacional.
c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim tek CSIRT-i kombëtar dhe aktorët e interesuar.

CSIRT pranë operatorit

a) Rikuperon shërbimet e prekura nga vulnerabilitetet e identifikuara, duke ndjekur planet e rikuperimit të vendosura.
b) Merr masa për sistemet e cilësuara si "pa mbështetje" **(*end-of-life*)**, si fortifikimi i tyre ose **micro-segmentimi** në rrjet.
c) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikuperuara përpara se të rifillojnë operacionet normale.
ç) Raporton progresin e rikthimit të shërbimeve dhe çdo problematikë drejt CSIRT-it kombëtar dhe atij sektorial për ndihmë të mëtejshme.

9.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport ku detajon vulnerabilitetet e identifikuara, veprimet e përgjigjes ndaj incidentit dhe rezultatet.
b) Rishikon aktivitetet pas incidentit për të nxjerrë mësime dhe për të evidentuar fushat që kanë nevojë për përmirësim në vlerësimet e ardhshme të vulnerabiliteteve.
c) Shpërndan raportet e analizimeve me CSIRT-in sektorial dhe atë pranëoperatorit për të rritur gadishmërinë e përgjithshme.

CSIRT Sektorial

a) Përgatit një raport për sektorin që përshkruan ndikimin e vulnerabiliteteve, veprimet e përgjigjes dhe përpjekjet e rikuperimit.

b) Merr pjesë në procesin e rishikimit të aktiviteteve pas incidentit, duke kontribuar me njohuri dhe rekomandime specifike për sektorin.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar vlerësimet e ardhshme të vulnerabiliteteve dhe aftësitë e përgjigjes.

CSIRT pranë operatorit

a) Harton një raport përfundimtar duke ofruar informacion të detajuar mbi ndikimin e vulnerabiliteteve, përgjigjen dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësime operacionale dhe duke përditësuar planet e përgjigjes.
c) Zbaton rekomandimet për të forcuar mbrojtjen dhe për të përmirësuar vlerësimet e ardhshme të vulnerabiliteteve.

10) Kriptominimi

Gjenerimi i kriptomonedhave është procesi i përdorimit të kompjuterave për të verifikuar dhe regjistruar transaksione në një rrjet *blockchain* për të fituar kriptovaluta, ky proces njihet si kriptominim. Kriptominimi cilësohet si incident kibernetik kur kryhet në mënyrë të paligjshme ose pa dijeninë e përdoruesve të një sistemi. Kjo ndodh kur sulmuesit instalojnë pa leje programe për të përdorur fuqinë përpunuese të kompjuterëve të viktimave për të gjeneruar monedha kriptografike, si Bitcoin, Etherium etj. Ky lloj sulmi, i njohur si "*cryptojacking*", mund të ngadalësojë sistemet, të konsumojë burime energjie dhe të dëmtojë pajisjet. Karakteristikat kryesore përfshijnë përdorimin e fshehtë të CPU ose GPU, përdorimin e kodeve të fshehura në faqet e internetit ose aplikacione dhe konsum të lartë të energjisë, pa pëlqimin e përdoruesit.

10.1 Përgatitja

CSIRT Kombëtar

a) Zhvillon politika dhe procedura për zbulimin dhe reagimin ndaj kërcënimeve si prodhimi kriptomonedhave, duke përfshirë kriptominimin e paautorizuar dhe kriptojacking.
b) Zbaton kontrolle të avancuara të sigurisë, duke pëdrorur sistemet e zbulimit të anomalive dhe mjetet e analizës së sjelljes, për të identifikuar aktivitete të kriptominimit.
c) Kryen trajnime të rregullta për analistët e CSIRT-it mbi teknikat më të fundit të kriptominimit, mjetet dhe trendet e fundit të gjenerimit të kriptomonedhave.
ç) Bashkëpunon me organizata ndërkombëtare të sigurisë kibernetike për të qëndruar të informuar mbi kërcënimet e fundit rreth kriptominimit.
d) Përcakton personat që do përfshihen në reagimin ndaj incidentit, rolet dhe përgjegjësitë për adresimin e vulnerabiliteteve.

CSIRT sektorial

a) Ofron udhëzime specifike për sektorin për identifikimin dhe zbutjen e kërcënimeve nga kriptominimi, duke siguruar përputhjen me strategjitë kombëtare.
b) Implementon teknologjitë dhe mjetet e monitorimit të përshtatura për të zbuluar përdorimin anormal të CPU/GPU/RAM dhe shenja të tjera të kriptominimit brenda sektorit.
c) Trajnon ekipet sektoriale të CSIRT mbi njohjen e treguesve të kriptominimit dhe protokollet e duhura të reagimit.

ç) Vendos politika për shkarkimin apo ekzekutimin e skedarëve apo skripteve vetëm nga përdoruesit me privilegje të larta.
d) Përditëson rregullisht konfigurimet e sigurisë për sektorin për të parandaluar aktivitetet e paautorizuara të kriptominimit.

CSIRT pranë operatorit
a) Implementon masa sigurie për të parandaluar kriptominimin, duke përfshirë mbrojtjen e pikave fundore, *patch*-e të rregullta dhe forcim të sistemeve.
b) Trajnon stafin mbi rreziqet e lidhura me kriptominimin, duke përfshirë ndikimin në performancën e sistemit dhe konsumin e energjisë.
c) Monitoron rregullisht performancën e sistemit dhe përdorimin e burimeve për të zbuluar shenja të kriptominimit të paautorizuar.
ç) Vendos protokolle për përshkallëzimin e shpejtë të incidentit të kriptominimit drejt CSIRT-eve përkatës.

10.2 Zbulimi

CSIRT Kombëtar
a) Monitoron vazhdimisht rrjetin kombëtar për shenja të aktiviteteve të kriptominimit, si përdorimi i pazakontë i CPU/GPU/RAM ose rritje të pashpjeguara në konsumin e energjisë.
b) Përdor burime të inteligjencës për kërcënimet dhe mjete për të analizuar sjelljen për të identifikuar aktivitetin e kriptominimit.
c) Bashkëpunon me CSIRT-in sektorial dhe atë pranë operatorit për të ndarë çdo të dhënë të zbuluar për të rritur ndërgjegjësimin mbi kërcënimet e kriptominimit.

CSIRT Sektorial
a) Implementon mjete monitorimi specifike në bazë të nevojave të sektorit për të zbuluar aktivitete të kriptominimit (përdorimi jonormal i burimeve kompjuterike ose trafik jo i zakontë në rrjet).
b) Shpërndan aktivitetet e zbuluara të kriptominimit me CSIRT-in kombëtar dhe CSIRT-et e tjera sektoriale për të koordinuar procesin e reagimit ndaj incidentit.
c) Asiston CSIRT-in pranë operatorit në monitorimin e sistemeve dhe rrjeteve specifike të sektorit për shenja të kriptominimit, duke përfshirë instalime të paautorizuara të software ose sjellje të pazakonta të sistemit.

CSIRT pranë operatorit
a) Përdor mjete monitorimi në sistemet fundore për të zbuluar softuerë të paautorizuar për kriptominim ose konsum anormal të burimeve.
b) Shikon sjelljen e sistemeve për konsum të CPU mbi normat normale. Operatori mund të përdori komandat **sudo top (*Linux*)** dhe përmes ***Task Manager*** (***Windows*)** për zbulimin e aktiviteteve që ndikojnë në ngarkimin e CPU.
c) Verifikohet konsumi i memorjes RAM, shikohen proceset që ngarkojnë memorjen përmes komandave **sudo free -h** (Linux) dhe përmes **Task Manager** > **Performance** (**Windows**)
ç) Hapsirën në disk përmes **This PC** (**Windows**) dhe **sudo df -h** (**Linux)**
d) Bandwithin nëse ka trafik të shtuar në rrjetin tuaj përmes programeve monitoruese
dh) Shikon për shfaqen e reklamave *pop-up* jashtë shfletuesit, ridrejtimi në faqje interneti të dëmshme apo instalimi i shtojcave pa miratimin e përdoruesit

e) Raporton menjëherë çdo aktivitet të zbuluar të kriptominimit tek CSIRT kombëtar dhe ai sektorial
ë) Ruan regjistrat dhe të dhënat e lidhura me aktivitetet e zbuluara të kriptominimit për analizim dhe përgjigje të mëtejshme.

10.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Konfirmon aktivitetin e kriptominimit si incident të sigurisë kibernetike përmes analizës së të dhënave të mbledhura dhe sjelljes së sistemit.
b) Identifikon shtrirjen dhe ndikimin e mundshëm të aktivitetit të kriptominimit në sigurinë kombëtare dhe gjitha infrastrukturat kritike dhe të rëndësishme.
c) Njofton CSIRT-in përkatës sektorial dhe atë pranë operatorit rreth aktivitetit të identifikuar të kriptominimit dhe implikimeve të tij të mundshme.

CSIRT Sektorial

a) Koordinon me CSIRT-in pranë operatorit aktivitetin e kriptominimit të raportuar nga vetë ata dhe vlerëson ndikimin e tij në asetet specifike të sektorit.
b) Koordinohet me operatorët për të përcaktuar shkallën e aktivitetit të kriptominimit brenda sektorit.
c) Ofron informacion të detajuar për incidentin drejt CSIRT-it kombëtar për një analizë të thelluar.

CSIRT pranë operatorit

a) Identifikon dhe dokumenton aktivitetin e kriptominimit, duke përfshirë teknikën, burimin dhe objektivat e mundshme.
b) Identifikon indikatorët**: IP, domain, hash-et** e skedarëve keqdashës.
c) Raporton incidentin drejt CSIRT-it kombëtar dhe atij sektorial, duke ofruar të gjitha evidencat përkatëse dhe analizën fillestare.

10.4 Komunikimi dhe

Koordinimi CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorëve.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT Sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për mbrojtje.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

10.5 Regjistrimi

CSIRT Kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidentit dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të mbledhur informacion shtesë dhe për të siguruar që incidenti të jetë i dokumentuar plotësisht.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur nga incidenti me qëllim regjistrimin e incidentit të kriptominimit brenda platformës së menaxhimit të incidenteve, duke siguruar që të gjitha të dhënat e mbledhura të jenë të regjistruara.
b) Koordinohet me CSIRT-in pranë operatorit me qëllim që të gjithë operatorët e prekur të jenë të përfshirë në procesin e regjistrimit.
c) Dërgon informacionet dhe detajet e incidentit të mbledhura drejt CSIRT-it kombëtar për të qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton incidentin e kriptominimit dhe çdo gjetje fillestare bazuar në të dhënat e mbledhura.
b) Siguron regjistrimin e duhur në sistemin e menaxhimit të incidenteve sipas përcaktimeve në rregulloren për kategorizimin e incidenteve të sigurisë kibernetike.
c) Raporton incidentin tek CSIRT-i sektorial dhe ai kombëtar me të gjitha detajet përkatëse.

10.6 Kategorizimi i

Incidentit CSIRT Kombëtar

a) Kategorizon aktivitetin e kriptominimit bazuar në natyrën, shtrirjen dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Klasifikon incidentin sipas ashpërsisë së tij, duke marrë parasysh dëmin e mundshëm në performancën e sistemit dhe konsumin e energjisë.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin si dhe ofron udhëzime për veprimet e duhura të përgjigjes.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit të kriptominimit brenda sektorit, bazuar në ndikimin e tij dhe të dhënat e mbledhura.
b) Ndihmon në përcaktimin e natyrës specifike të kriptominimit dhe rëndësinë e tij për operacionet sektoriale.

CSIRT pranë operatorit

a) Kategorizon dhe raporton incidentin e kriptominimit, duke siguruar që të gjitha informacionet në dispozicion ndihmojnë në kategorizimin e incidentit.
b) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.
c) Zbaton masa të menjëhershme për të zbutur çdo dëm të shkaktuar nga aktiviteti i kriptominimit.

10.7 Prioritizim i incidentit

CSIRT Kombëtar

a) Vlerëson ndikimin e aktivitetit të kriptominimit bazuar në potencialin e tij për të rritur kostot e infrastrukturës (konsum i lartë i energjisë elektrike), ndërprerë shërbimet kritike ose për të kompromet uar performancën e sistemit.
b) Prioritizon përgjigjen ndaj incidentit, duke i dhënë përparësi incidentit që mund të çojë në ndërprerje të rëndësishme operacionale.
c) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që incidentet më kritike të trajtohen me shpejtësi.

CSIRT Sektorial

a) Vlerëson ndikimin e aktivitetit të kriptominimit në shërbimet kritike të sektorit dhe prioritizon sipas nevojës.
b) Koordinon me CSIRT-in pranë operatorit prioritizimin, me qëllim sinkronizimin e përgjigjes ndaj incidentit.
c) Asiston CSIRT-in pranë operatorit me qëllim zbutjen e kërcënimeve më të afërta dhe më të rënda të identifikuara përmes incidentit të kriptominimit.

CSIRT pranë operatorit

a) Vlerëson ndikimin e aktivitetit të kriptominimit në proceset operacionale dhe prioritizon veprimet e përgjigjes sipas nevojës.
b) Siguron që çdo ndërprerje e mundshme e shërbimeve ose degradim i performancës të menaxhohet dhe adresohet menjëherë.
c) Raporton vendimet për prioritizim tek CSIRT-i kombëtar dhe ai sektorial, duke ofruar analizime dhe arsyetime.

10.8 Analiza e Incidentit

CSIRT Kombëtar

a) Kryen analizë të plotë të aktivitetit të kriptominimit, duke u fokusuar në burimin, metodën dhe ndikimin e mundshëm në sigurinë kombëtare.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur informacione dhe detaje shtesë mbi teknikat e kriptominimit.
c) Analizon dhe shpërndan indikatorët e kompromentimit në të gjitha infrastrukturat kritike dhe të rëndësishme.
ç) Shpërndan raportin pas analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në reduktimin e kohës së përgjigjes dhe në përpjekjet e parandalimit të incidenteve të ngjashme në të ardhmen.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në analizimin e incidentit duke shfrytëzuar informacionet e mbledhura nga raportimet e operatorit dhe nga platformat e inteligjencës së kërcënimeve dhe shikon për indikatorët e kompromentimit në të gjithë sektorin, me qëllim shmangien e incidentit.
b) Analizon si u arrit deri në kompromentimin e sistemit që të shfrytëzohej për gjenerimin e kriptomonedhave dhe sugjeron strategji për marrjen e masave nga incidentit.
c) Shpërndan detaje nga analiza e kryer drejt operatorëve dhe CSIRT-it kombëtar për të ofruar informacion të detajuar rreth incidentit.

CSIRT pranë operatorit

a) Analizon aktivitetin e kriptominimit në nivel operativ, duke u fokusuar në mënyrën se si mund të ndikojë në sistemet dhe shërbimet kritike.
   - Psh: Pajisjet fillojnë të funksionojnë më ngadalë se zakonisht, sepse përdor burimet maksimale të kompjuterit. Kjo çon në vonesën e egzekutimit të komandave dhe egzekutimin me vështirësi të disa programeve paralelisht.
   - Rritja e papritur e kostove të energjisë.
   - Monitoroni CPU, nëse punon 80-90% kur nuk keni egzekutuar asnjë program, është një indicie që kompjuteri juaj mund të jetë i infektuar.
   - Pajisjet e infektuara me gjenerues kriptovalutash, tentojnë të nxehen duke qenë se përdorin shumë CPU, mund të zvogëlojnë kohën e baterisë, si dhe në raste specifike mund të dëmtojnë pajisjet.
   - Shfaqja e reklamave pop-up jashtë shfletuesit, ridrejtimi në faqje interneti të dëmshme, instalimi i shtojcave pa miratimin e përdoruesit.
b) Shpërndan gjetjet me CSIRT-et për të kontribuar në një kuptim më të gjerë rreth incidentit të identifikuar si kriptominim.
c) Analizon log-et për të gjetur pikën e hyrjes, dhe të gjithë indikatorët që ndikojnë në kompromentimin e sistemit.
ç) Zbaton gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar incidente të ngjashme të kriptominimit.

10.9 Izolimi dhe fshirja

CSIRT Kombëtar

a) Ofron udhëzime dhe mbështetje për zbutjen e ndikimit të aktiviteteve të identifikuara të kriptominimit.
b) Koordinon përpjekjet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që strategjitë e qëndrueshmërisë kibernetike të zbatohen në të gjitha sektorët.
c) Asiston operatorët e infrastrukturave të informacionit në procesin e fshirjes të të gjithë indikatorëve që lidhen me aktivitetin e kriptominimit.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në marrjen e masave parandaluese në të gjithë sektorin për të shmangur aktivitete të mëtejshme të kriptominimit.
b) Koordinohet me operatorët për të siguruar eliminimin efektiv të softuerëve apo skripteve të kriptominimit dhe për të rikthyer sistemet e prekura.

c) Monitoron situatën për të siguruar që të gjithë indikatorët e identifikuar të adresohen dhe incidenti të jetë zgjidhur plotësisht.

CSIRT pranë operatorit

a) Izolon sistemet e prekura dhe rrjetin me të cilin këto sisteme komunikojnë.
b) Ndjek procedurat e eliminimit të indikatorëve të kompromentimit që ofrohen nga CSIRT-i kombëtar dhe ai sektorial, duke siguruar që të gjitha hapat e nevojshëm të ndërmerren.
c) Bllokon të gjithë indikatorët në pajisjet mbrojtëse, dhe monitoron në vazhdim trafikun për prezencën e këtyre indikatorëve në sisteme të tjera.
   i. Është i rëndësishëm izolimi i skedarit që gjeneron kriptovalutat, në mënyrë që mos shpërndahet në rrjet. Për këtë duhet të bëni skanime të herë pas hershme të pajisjeve.
   ii. Përditësoni antivirusin dhe skanoni të gjithë pajisjen për të identifikuar dhe fshirë skedarin
   iii. Disa gjenerues kriptomonedhash operojnë në shfletues dhe vendosin script në cache ose cookies. Duhet të fshini të dhënat e shfletuesit, fotot, skedarët dhe cookies.
   iv. Resetoni të gjitha konfigurimet e shfletuesit, dhe instaloni manualisht vetëm shtojcat që ju duhen.
   v. Shkëpusni përkohësisht internetin në mënyrë që të ndërprisni komunikimin.
   vi. Përdorni vetëm antiviruse të besuara.
   vii. Aktivizoni dhe konfiguroni firewall pë të bllokuar akseset e paautorizuara.
   viii. Shmangni linket jo të besuara, shkarkoni programet vetëm nga faqe të besuara, mos shkarkoni bashkëlidhjet nga dërgues të panjohur dhe gjithmonë kontrolloni URL para se ta klikoni.
ç) Verifikon efektivitetin e masave të marra dhe raporton statusin drejt CSIRT-eve.

10.10 Rikthimi i shërbimeve / të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e çdo shërbimi të prekur nga aktiviteti i kriptominimit në operacione normale.
b) Koordinohet me CSIRT-et sektoriale dhe ato pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Monitoron sistemet gjatë dhe pas rikuperimit për të siguruar stabilitetin dhe për të parandaluar incidente të ardhshme.

CSIRT Sektorial

a) Asiston CSIRT pranë operatorit në rikuperimin e shërbimeve sektoriale, duke prioritizuar shërbimet ose sistemet më kritike dhe të prekura.
b) Mbështet CSIRT-it pranë operatorit në rikthimin e shërbimeve në kapacitetin e plotë operacional.
c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim tek CSIRT-i kombëtar dhe aktorët e interesuar.

CSIRT pranë operatorit

a) Fillon procesin e rikuperimit për shërbimet e prekura nga aktiviteti i kriptominimit, duke ndjekur planet e rikuperimit të vendosura:

i. Përdorimi i produkteve antivirus që mbrojnë sistemin nga gjenerimi i kriptomonedhave dhe mbajini ato të azhornuara.
ii. Kontrolli i faqeve të internetit për kodet e gjenerimit të kriptomonedhave, pasi kjo mund të dëmtojë reputacionin e tyre kur klientët bëhen viktima. Për këtë qëllim, administratorët e faqeve të internetit duhet të bëjnë kontrolle të rregullta për ndryshime të dyshimta të faqes së internetit ose ndonjë ndryshim në server.
iii. ***Çaktivizimi i JavaScript*** kur hapni faqe të dyshimta ose të pa njohura të internetit.
iv. Mos lejimi i ***macro*** në Microsoft Word nëse nuk është e nevojshme.
v. Përdorimi i versioneve të azhornuara të shfletuesve të internetit.
vi. Përditësimi me lajmet e gjenerimit të kriptomonedhave, trendet dhe kërcënimet, për të qenë në gjendje për t'i identifikuar paraprakisht.

b) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikthyera para se të rifilloj operacionet normale.
c) Raporton progresin e rikuperimit dhe çdo sfidë tek CSIRT-i kombëtar dhe ai sektorial për ndihmë të mëtejshme.

10.11 Aktiviteti pas incidentit

CSIRT kombëtar

a) Harton një raport të detajuar mbi incidentin e kriptominimit, veprimet e përgjigjes dhe rezultatet.
b) Rishikon aktivitetet pas incidentit për të nxjerrë mësime dhe për të evidentuar aspektet që kanë nevojë për përmirësim duke filluar nga përgatitja deri në rikthimin e shërbimeve dhe të dhënave.
c) Shpërndan raportet e analizimeve me CSIR-et sektoriale dhe ato pranë operatorëve për të rritur gatishmërinë e përgjithshme.

CSIRT sektorial

a) Përgatit një raport për sektorin specifik ku përshkruan incidentin e kriptominimit, veprimet e përgjigjes dhe përpjekjet e rikuperimit.
b) Merr pjesë në procesin e rishikimit të aktiviteteve pas incidentit, duke kontribuar me njohuri dhe rekomandime specifike për sektorin
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar zbulimin dhe kohen e përgjigjes në incidente të ngjashme në të ardhmen.

CSIRT pranë operatorit

a) Harton një raporti përfundimtar duke ofruar informacion të detajuar mbi ndikimin e incidentit të kriptominimit në sisteme dhe në operacionet e operatorit, përgjigjen dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësime operacionale dhe duke përditësuar planet e përgjigjes.
c) Zbaton rekomandimet për të forcuar mbrojtjet dhe për të përmirësuar zbulimin e ardhshëm të aktiviteteve të kriptominimit.

11) Rrjedhja e të dhënave

Rrjedhja e të dhënave është një incident kibernetik, ku informacioni sensitiv është kompromentuar ose zbuluar pa lejen e duhur.
Në këtë situatë, një sulmues ose një grup sulmuesish ka fituar qasje të paligjshme në sistemet ose në bazën e të dhënave të një infrastrukture dhe ka arritur të kopjojë, zhvendosë, ose publikojë informacionin e vjedhur.
Kjo kategori incidenti prek të dhënat personale, financiare dhe integritetin e një organizate, si dhe kërkonë një reagim të menjëhershëm për të parandaluar më shumë dëme dhe për të identifikuar burimin dhe pasojat e rrjedhjes së të dhënave.

11.1 Përgatitja

CSIRT kombëtar

a) Harton dhe mirëmban politika dhe procedura për zbulimin dhe reagimin ndaj incidenteve të rrjedhjes së të dhënave.
b) Përdor platforma inteligjente që ndihmojnë në evidentimin e rrjedhjes së të dhënave për të gjithë infrastrukturat kritike dhe të rëndësishme të informacionit në rrjetet kombëtare.
c) Trajnon rregullisht analistët e CSIR-ve mbi identifikimin e teknikave të marrjes së të dhënave (*eksfiltrimit*), duke përfshirë metodat më të fundit të përdorura nga aktorët keqdashës.
ç) Siguron që mjetet dhe sistemet për zbulimin dhe parandalimin e eksfiltrimit të të dhënave (DLP, IDS/IPS) janë të implementuara dhe funksionale në nivel kombëtar.
d) Bashkëpunon me organizata ndërkombëtare të sigurisë kibernetike për të qëndruar të informuar mbi kërcënimet e reja të eksfiltrimit dhe praktikat më të mira për zbulimin dhe mbrojtjen nga këto sulme.
dh) Përcakton personat që do të menaxhojnë incidentin dhe përcakton rolet dhe përgjegjësitë e tyre.

CSIRT Sektorial

a) Ofron udhëzime për sektorin për mbrojtjen kundër eksfiltrimit të të dhënave, duke siguruar përputhjen me strategjitë kombëtare.
b) Koordinohet me CSIRT-in pranë operatorit me qëllim përdorimin e mjeteve të monitorimit si (DLP/IDS/IPS) të përshtatura për të zbuluar transferime të pazakonta të të dhënave, akses të paautorizuar dhe aktivitete të mundshme të eksfiltrimit.
c) Trajnon ekipet sektoriale të CSIRT mbi njohjen e shenjave të eksfiltrimit të të dhënave dhe hapat që duhen marrë për reagimin ndaj incidentit.
ç) Identifikon dhe siguron asetet më kritike të sektorit, që mund të jenë shënjestër për rrjedhjen e të dhënave.
d) Koordinohet me operatorët me qëllim përditësimin rregullisht të konfigurimeve të sigurisë për paisjet e mbrojtjes (firewall) lidhur me kërcënimet më të reja mbi marrjen e të dhënave.

CSIRT pranë operatorit

a) Zbaton kontrolle të forta aksesi, kriptimi dhe implementon sisteme mbrojtëse si DLP për të parandaluar eksfiltrimin e paautorizuar të të dhënave.
b) Trajnon stafin mbi rreziqet e lidhura me eksfiltrimin e të dhënave, duke përfshirë rëndësinë e respektimit të politikave të sigurisë së të dhënave.
c) Monitoron rregullisht transferimet e të dhënave dhe trafikun në rrjet për të zbuluar aktivitete të pazakonta që mund të tregojnë përpjekje për eksfiltrim.
ç) Aplikon politika dhe procedura për:
   i. Priviligjet e përdoruesve në aksesimin e të dhënave.
   ii. Kriptimin e të dhënat të ndjeshme.
   iii. Transferimin e të dhënave në mënyrë të sigurt.
d) Ruan kopje rezervë të të dhënave kritike për të rikthyer shërbimet në rast incidenti të rrjedhjes së të dhënave.

11.2 Zbulimi

CSIRT Kombëtar

a) Monitoron vazhdimisht rrjetet kombëtare për shenja të eksfiltrimit të të dhënave, si transferime të mëdha ose të pazakonta të të dhënave, akses të paautorizuar, ose përdorimin e kanaleve të komunikimit jo-standard.
b) Përdor burime të inteligjencës për kërcënimet dhe mjete të analizës së sjelljes për të identifikuar aktivitete të mundshme të eksfiltrimit.

CSIRT sektorial

a) Koordinohet me CSIRT-in pranë operatorit me qëllim përdorimin e mjeteve të monitorimit specifike për sektorin për të zbuluar aktivitete të eksfiltrimit, si rrjedha e të dhënave ose akses të paautorizuar në informacionin sensitive.
b) Ndan aktivitetet e zbuluara të eksfiltrimit me CSIRT kombëtar dhe CSIRT e tjera sektoriale për përpjekje të koordinuara të reagimit.
c) Asiston CSIRT-in pranë operatorit në monitorimin e sistemeve dhe rrjeteve specifike të sektorit për shenja të rrjedhes së të dhënave, duke përfshirë instalime të paautorizuara të software ose sjellje të pazakonta të sistemit.

CSIRT pranë operatorit

a) Përdor mjete për monitorimin e sistemeve fundore dhe rrjetit për të zbuluar transferime të paautorizuara të të dhënave ose aktivitete të dyshimta që mund të tregojnë eksfiltrim.
b) Implementon dhe përdor **YARA Rules** për të zbuluar skedarë të dyshimtë që lidhin komunikimin me aktorët keqdashës dhe që çojnë në rrjedhjen e të dhënave.
c) Monitoron veprimet e personave të brendshëm me akses në të dhënat kritike, duke kontrolluar për sjellje të pazakonta, si:
   i. Transferimi i të dhënave në pajisje të jashtme (USB, disqe të lëvizshme).
   ii. Aksesimi i të dhënave jashtë orarit të punës ose nga vendndodhje të pazakonta.
   iii. Ndryshimi i privilegjeve të përdoruesit pa autorizim të duhur.

ç) Raporton menjëherë çdo aktivitet të zbuluar të eksfiltrimit drejt CSIRT-it kombëtar dhe atij sektoriale.
d) Ruani loge-et dhe të dhënat e lidhura me aktivitetet e zbuluara të eksfiltrimit për analizim dhe përgjigje ndaj incidentit.

11.3 Identifikimi i incidentit

CSIRT kombëtar

a) Konfirmon prezencën e rrjedhjes së të dhënave përmes analizës së thelluar, duke shfrytëzuar burimet kombëtare të inteligjencës.
b) Identifikon shtrirjen dhe ndikimin e mundshëm të eksfiltrimit të të dhënave në infrastrukturat kritike dhe të rëndësishme në të gjithë vendin.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për incidentin e rrjedhjes së të dhënave dhe për pasojat e mundshme.

CSIRT sektorial

a) Koordinon me CSIRT-in pranë operatorit lidhur me raportimin e incidentit të rrjedhjes së të dhënave të bërë nga operatorët dhe vlerëson ndikimin e tij në asetet e sektorit.
b) Koordinohet me operatorët për të përcaktuar sasinë e të dhënave që kanë rrjedhur brenda sektorit.
c) Ofron informacion të detajuar për incidentin drejt CSIRT-it kombëtar për një analizë të thelluar.

CSIRT pranë operatorit

a) Identifikon aktivitetet e pazakonta nga persona të brendshëm duke përfshirë, por pa u kufizuar vetëm në:
   i. Transferimin e madh të të dhënave në pajisje të lëvizshme (USB, disqe të jashtme) ose platforma cloud.
   ii. Aksesimin e të dhënave jashtë orarit të punës ose nga vendndodhje të pazakonta.
   iii. Krijimin ose ndryshimin e privilegjeve të përdoruesit pa autorizim të dokumentuar.
b) Për çdo aktivitet të pazakontë të zbuluar, operatori duhet të nisë një hetim të brendshëm për të identifikuar burimin e mundshëm të rrjedhjes dhe të zbatojë masa të menjëhershme për të parandaluar eksfiltrimin e mëtejshëm.
c) Identifikon dhe dokumenton aktivitetin e eksfiltrimit, duke përfshirë metodën, burimin dhe objektivat e mundshme.
ç) Identifikon aktivitetetet e pazakonta nga jashtë duke përfshirë, por pa u kufizuar vetëm në:

i. Trafik të pazakontë në rrjet, veçanërisht drejt IP-ve të panjohura ose domain-eve të dyshimta.
ii. Aksesimin e burimeve të brendshme nga adresat IP të jashtme në periudha të pazakonta.
iii. Përpjekjet për transferimin e të dhënave në destinacione të jashtme pa autorizim.

d) Raporton incidentin tek CSIRT-i kombëtar dhe ai sektorial, duke ofruar të gjitha të dhënat përkatëse dhe analizën fillestare.
dh) Verifikon nëse rrjedhja ka ndodhur përmes kanaleve të ndryshme (email, cloud, etj.) si dhe raporton tek CSIRT-i kombëtar dhe ai sektorial me informacione të detajuara.
e) Identifikon qëllimin e aktivitetit të eksfiltrimit dhe ndikimin e tij të mundshëm në operacionet.

11.4 Komunikimi dhe Koordinimi

CSIRT Kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe CSIRT-it pranë operatorit.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Njofton regullisht CSIRT-in pranë operatorit për rrjedhje të të dhënave të identifikuara përmes sistemeve inteligjete dhe kërkimet e thelluara në *dark web.*
ç) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për reagim.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

11.5 Regjistrimi

CSIRT kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidenteve, së bashku me detajet e rrjedhjes së të dhënave.

b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të mbledhur informacionin e nevojshëm dhe për të siguruar që incidenti është dokumentuar plotësisht.

CSIRT sektorial

a) Koordinohet me CSIRT-in pranë operatorit të prekur nga incidenti me qëllim regjistrimin e incidentin në platformën e menaxhimit të mundësuar nga CSIRT-i kombëtar dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Dërgon informacionin e mbledhur drejt CSIRT-it kombëtar për të qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton incidentin e eksfiltrimit dhe çdo gjetje fillestare bazuar në të dhënat e mbledhura.
b) Siguron regjistrimin e duhur në sistemin e menaxhimit të incidenteve sipas përcaktimeve të rregullores për kategorizimin e incidenteve të sigurisë kibernetike.
c) Raporton incidentin tek CSIRT-i kombëtar dhe ai sektorial me të gjitha detajet përkatëse.

11.6 Kategorizimi i Incidentit

CSIRT kombëtar

a) Kategorizon incidentin si "rrjedhje e të dhënave" bazuar në analizimin e kërcënimit dhe llojin e të dhënave të kompromentuara.
b) Klasifikon incidentin sipas ashpërsisë dhe ndikimit të tij në sigurinë kombëtare, privatësinë e qytetarëve dhe funksionalitetin e infrastrukturës kritike.
c) Njofton CSIRT-in sektorial dhe atë pranë operatorit për kategorizimin dhe jep rekomandimet e nevojshme për veprimet e duhura të përgjigjes.

CSIRT Sektorial

a) Koordinohet me CSIRT-in pranë operatorit në lidhje me kategorizimin e incidentit dhe e komunikon atë brenda sektorit përkatës.
b) Siguron që operatorët të ndjekin procedurat e përcaktuara për menaxhimin e rrjedhjes së të dhënave.
c) Ndihmon në përcaktimin e natyrës së saktë të incidentit dhe të dhënave të kompromentuara.

CSIRT pranë operatorit

a) Kategorizon dhe raporton incidentin dhe siguron që të gjitha informacionet ndihmojnë në kategorizimin e tij.
b) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.
c) Zbaton masa të menjëhershme për të zbutur ndikimin e rrjedhjes së të dhënave.

11.7 Prioritizim i incidentit

CSIRT Kombëtar

a) Vlerëson rëndësinë e informacionit që ka rrjedhur bazuar në ndikimin e mundshëm të tij në infrastrukturën kombëtare.

b) Prioritizon përgjigjen ndaj incidentit, duke u fokusuar në ato raste që kanë potencial të lartë për të shkaktuar dëme në sisteme apo shërbime kritike.
c) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që incidentet më kritike të trajtohen me shpejtësi.

CSIRT Sektorial

a) Vlerëson ndikimin e aktivitetit në shërbimet kritike të sektorit dhe prioritizon sipas nevojës.
b) Koordinon me CSIRT-in pranë operatorit prioritizimin e incidentit, duke siguruar një koordinim të përshtatshëm për përgjigjen ndaj rrjedhjes së të dhënave.
c) Asiston CSIRT-in pranë operatorit me qëllim zbutjen e kërcënimeve më ndikimin më të lartë bazuar në vlerësimin e shërbimeve kritike.

CSIRT pranë operatorit

a) Vlerëson ndikimin e rrjedhjes së të dhënave në shërbimet operacionale dhe prioritizon veprimet e reagimit sipas rrezikshmërisë së tij.
b) Siguron që çdo ndërprerje e mundshme e shërbimeve të jetë menaxhuar dhe adresuar menjëherë.
c) Raporton vendimet për prioritizim drejt CSIRT kombëtar dhe atij sektorial, bazuar në analizime dhe arsyetime të sakta.

11.8 Analiza e Incidentit

CSIRT Kombëtar

a) Kryen analizën forensike për të kuptuar origjinën, mënyrën e ekzekutimit dhe ndikimin e rrjedhjes së të dhënave.
b) Bashkëpunon me partnerët ndërkombëtarë dhe agjencitë e inteligjencës për të mbledhur më tepër informacion mbi teknikat dhe mjetet e përdorura për eksfiltrimin e të dhënave.
c) Shpërndan rezultatet e analizës me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në parandalimin e incidenteve të ngjashme në të ardhmen.

CSIRT Sektorial

a) Asisiton CSIRT-in pranë operatorit në analizimin e aktivitetit të eksfiltrimit, duke shfrytëzuar informacionet e mbledhura nga platformat inteligjente të kërcënimeve apo nga informacionet e vendosura në dispozicion nga operatorët.
b) Asiston CSIRT-in pranë operatorit në identifikimin e dobësive të shfrytëzuara që kanë çuar në rrjedhjen e të dhënave si dhe sugjeron strategj për zbutjen e ndikimit.
c) Siguron shpërndarjen e raportit të analizës tek CSIRT-i kombëtar për të qartësuar situatën.

CSIRT pranë operatorit

a) Analizon aktivitetin e eksfiltrimit në nivel operativ, duke u fokusuar në mënyrën se si mund të ndikojë në sistemet dhe shërbimet kritike.
b) Mbledh dhe analizon log-et për të gjurmuar veprimtaritë e dyshimta dhe identifikon metodat e përdorura për eksfiltrimin e të dhënave.

c) Analizon log-et nga sistemet kritike dhe pajisjet e rrjetit për shenja të kompromentimit, duke përfshirë:
   i. Përpjekjet e aksesimit të të dhënave pa autorizim;
   ii. Proceset që krijojnë lidhje të fshehta drejt IP-ve të panjohura;
   iii. Modifikimi i të dhënave ose kopjimi i skedarëve të ndjeshëm;

ç) Analizon për procese të dyshimta në sistem për të identifikuar aplikacionet e mundshme që përdoren për eksfiltrimin e të dhënave

d) Shpërndan gjetjet me CSIRT-in sektorial dhe atë kombëtar për të kontribuar në një kuptim më të gjerë të incidentit të eksfiltrimit.

dh) Shfrytëzon gjetjet për të përmirësuar masat e sigurisë dhe për të parandaluar përpjekjet e mëtejshme për eksfiltrim.

11.9 Izolimi dhe fshirja

CSIRT Kombëtar

a) Ofron udhëzime dhe mbështetje për zbutjen e ndikimit të aktiviteteve të identifikuara si rrjedhje e të dhënave.

b) Koordinon reagimin me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të zbatohen strategjitë e qëndrueshmërisë kibernetike nga të gjitha sektorët.

c) Adreson çdo dobësi të shfrytëzuar nga aktiviteti i eksfiltrimit, duke siguruar reduktimin dhe parandalimin e rasteve të ngjashme në të ardhmen.

d) Shpërndan drejt CSIRT-it pranë operatorëve indikatorët e kompromentimit (IP/skedarë/url) të nxjerra nga analizimi i të dhënave të mbledhura nga operatorët dhe CSIRT-i sektrorial.

CSIRT Sektorial

a) Koordinon me CSIRT-in pranë operatorit me qëllim implementimin e masave mbrojtëse në të gjithë sektorin për të parandaluar aktivitete të mëtejshme të eksfiltrimit.

b) Punon ngushtë me operatorët për të siguruar fshirjen e kërcënimit nga sistemet dhe për të rikthyer sistemet e prekura.

c) Monitoron situatën për tu siguruar që të gjitha dobësitë e identifikuara janë adresuar dhe incidenti është zgjidhur plotësisht.

CSIRT pranë operatorit

a) Izolon çdo sistemet bazuar në prioritizim, për të ndaluar eksfiltrimin e mëtejshëm të të dhënave.

b) Çaktivizon përdoruesit të cilët po kryejnë aktivitet të dyshimtë.

c) Bllokon komunikimet me IP keqdashëse të identifikuar përmes analizimeve dhe të raportuara nga CSIRT-i kombëtar dhe ai sectorial.

ç) Ndjek procedurat që vendosen në dispoziocion nga CSIRT-i kombëtar dhe ai sektorial për fshirjen e indikatorëve të kompromentimit, ose fshirjen e sistemit.

d) Verifikon që aktiviteti nuk është më prezent në sistem dhe raporton statusin tek CSIRT-i kombëtar dhe ai sektorial.

11.10 Rikthimi i shërbimeve / të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e çdo shërbimi të prekur nga aktiviteti i eksfiltrimit në operacione normale.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Monitoron sistemet gjatë dhe pas rikthimit për të siguruar që aktiviteti keqdashës është zhdukur dhe parandalimin e tij në të ardhmen.

CSIRT sektorial

a) Ndihmon në rikthimin e shërbimeve sektoriale, duke prioritizuar shërbimet ose sistmet më kritike të prekura.
b) Mbështet operatorët në rikthimin e shërbimeve në kapacitetin e plotë operacional.
c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim drejt CSIRT-it kombëtar dhe aktorët e interesuar.

CSIRT pranë operatorit

a) Rikthen shërbimet e prekura nga aktiviteti i eksfiltrimit, duke ndjekur planet e rikuperimit të vendosura.
b) Riaktivizon përdoruesit e çaktivizuar, duke ndryshuar fillimisht fjalëkalimin e tyre.
c) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikuperuara përpara se të rifillojnë operacionet normale.
ç) Raporton progresin e rikuperimit dhe çdo problematikë të shfaqur gjatë rikthimit të shërbimeve drejt CSIRT-it kombëtar dhe atij sektorial për ndihmë të mëtejshme.

11.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport të plotë që detajon incidentin e eksfiltrimit, veprimet e përgjigjes dhe rezultatet.
b) Rishikon aktivitetet pas incidentit për të nxjerr mësime dhe për të evidentuar fushat që kanë nevojë për përmirësim për të shmangur rastet e ngjashme të rrjedhjes së të dhënave.
c) Shpërndan raportin përfundimtar me CSIRT-in sektorial dhe atë pranë operatorit për të rritur gatishmërinë e përgjithshme.

CSIRT Sektorial

a) Përgatit një raport për sektorin specifik dhe përshkruan ndikimin e incidentit të eksfiltrimit, veprimet e përgjigjes dhe përpjekjet e rikuperimit.
b) Merr pjesë në procesin e rishikimit pas incidentit, duke kontribuar me njohuri dhe rekomandime specifike për sektorin.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar zbulimin dhe aftësitë e përgjigjes në të ardhmen.

CSIRT pranë operatorit

a) Harton një raport përfundimtar duke ofruar informacion të detajuar mbi ndikimin e incidentit të eksfiltrimit, përgjigjen dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësime operacionale dhe duke përditësuar planet e përgjigjes.
c) Zbaton rekomandimet për të forcuar mbrojtjen dhe për të përmirësuar zbulimin e ardhshëm të aktiviteteve të eksfiltrimit.

12) Të tjera

Të tjera përfshin incidente të sigurisë së informacionit që nuk bëjnë pjesë në kategoritë e sipër përmendura. Kjo mund të përfshijë incidente të veçanta ose të pazakonta siç mund të jenë incidentet: dështimi i sistemit "*System Failure*", incidente nga fatkeqësitë natyrore, incidentet të lidhura me palë të treta etj.

12.1 Përgatitja

CSIRT kombëtar

a) Harton politika dhe udhëzime për menaxhimin e incidenteve të pazakonta, duke përfshirë dështimin e sistemeve apo incidentet zinxhir që vijnë si pasojë e kompromentimit të palëve të treta.
b) Siguron që të gjithë CSIRT-et sektoriale dhe ato pranë operatorëve të kenë një plan të detajuar të vazhdimësisë së biznesit për raste të dështimit të sistemit në infrastrukturën e tyre.
c) Organizon trajnime dhe ushtrime për skenarë incidentesh "Të tjera" për të përmirësuar kohën e reagimit dhe rikuperimit për rikthimin e shërbimeve.
ç) Përcakton personat që do të menaxhojnë incidentin dhe përcakton rolet dhe përgjegjësitë e tyre.

CSIRT sektorial

a) Harton procedura për monitorimin e performancës së shërbimeve të palëve të treta dhe sistemeve kritike në sektor.
b) Koordinon me CSIRT-in pranë operatorit me qëllim implementimin e sistemeve që paralajmërojnë për dështime të mundshme të sistemit dhe ngjarje të pazakonta.
c) Koordinohet me operatorët me qëllim krijimin e një plani reagimi për të minimizuar ndikimin e incidentit, si ndërprerja e shërbimeve të palëve të treta ose defektet e sistemeve.

CSIRT pranë operatorit

a) Zhvillon dhe mban një inventar të përditësuar të komponentëve hardware dhe software që janë të varura nga palët e treta.
b) Përgatit planin e rikuperimit për raste të dështimit të sistemit dhe incidentet e lidhura me furnizuesit e jashtëm.
c) Bashkëpunon dhe lidh marrëveshje me furnizuesit e palëve të treta për të siguruar reagim të shpejtë në rastet e incidenteve.

12.2 Zbulimi

CSIRT kombëtar

a) Përdor sisteme inteligjente për njoftimin e rënies së shërbimit të kompanive që funksionojnë si palë të treta në nivel kombëtar.
b) Analizon raportimet nga CSIRT-i sektorial dhe ai pranë operatorit për të identifikuar nëse incidenti është një problem më i gjerë në nivel kombëtar.

CSIRT sektorial

a) Asiston CSIRT-in pranë operatorit në monitorimin e performancës së shërbimeve kritike dhe aplikacioneve për të zbuluar shenjat e hershme të dështimit të sistemit.
b) Asiston CSIRT-in pranë operatorit lidhur me mjetet e monitorimit të përdorura për të identifikuar kur shërbimet e palëve të treta bëhen të papërdorshme ose funksionojnë nën standardet e pritura.

CSIRT pranë operatorit

a) Monitoron sistemet dhe aplikacionet për të zbuluar çdo dështim të papritur ose gabime që mund të ndikojnë në funksionimin e infrastrukturës
b) Kontrollon rregullisht marrëdhëniet me furnizuesit e palëve të treta për të identifikuar çdo njoftim për ndërprerje ose probleme të mundshme.
c) Konfiguron paralajmërime për të zbuluar dështimet e pajisjeve hardware dhe probleme të tjera që ndikojnë në funksionimin normal.

12.3 Identifikimi i incidentit

CSIRT Kombëtar

a) Analizon të dhënat e sistemit dhe raportimet nga CSIRT-i sektorial dhe ai pranë operatorit për të përcaktuar natyrën e incidentit dhe impaktin e mundshëm në infrastrukturat kritike.
b) Vlerëson nëse problemi lidhet me dështime të brendshme të sistemit, mos funksionim i të palëve të treta, ose me një incident nga fatkeqësitë natyrore.

CSIRT Sektorial

a) Kontrollon dhe verifikon raportimet e dështimit të sistemeve ose incidenteve të palëve të treta nga operatorët.
b) Analizon log-et e sistemeve për të identifikuar shkaqet dhe ndikimin e incidentit në sektor
c) Mbledh të dhëna nga operatorët për të vlerësuar se si ndikimi i incidentit mund të përhapet në sektorin përkatës.

CSIRT pranë operatorit

a) Identifikon burimin e problemit, siç janë gabimet hardware, software, ose ndërprerjet nga furnizuesit e palëve të treta.
b) Analizon log-et e sistemit dhe raportet e palëve të treta për të kuptuar shkaqet e incidentit.

c) Verifikon funksionalitetin e pajisjeve dhe sistemeve për të identifikuar komponentët që janë të prekur.

12.4 Komunikimi dhe Koordinimi

CSIRT kombëtar

a) Vendos kanale komunikime midis CSIRT-it kombëtar, CSIRT-it sektorial dhe atij pranë operatorit.
b) Ofron përditësime dhe udhëzime kohë pas kohe për të gjitha palët përkatëse gjatë incidentit.
c) Koordinon veprimet për reagimin ndaj incidentit duke ndjekur një mënyrë të unifikuar për zbutjen e tij.

CSIRT sektorial

a) Shfrytëzon informacionet paraprake të ofruara nga operatorët dhe i raporton drejt CSIRT-it kombëtar.
b) Koordinohet drejtpërdrejt me operatorët për të siguruar që informacionet kritike rreth incidentit të ndahen në kohë sa më të shpejtë dhe me saktësi për të optimizuar përgjigjen operacionale.
c) Kryen takime të rregullta me operatorët dhe CSIRT-et e tjera sektoriale për të harmonizuar veprimet dhe për të përditësuar strategjitë e mbrojtjes gjatë incidentit.

CSIRT pranë operatorit

a) Koordinohet me departamentet e tjera brenda infrastrukturës, duke siguruar që të gjitha palët përkatëse të jenë në dijeni të situatës dhe të marrin masa të përshtatshme për reagim.
b) Informojnë në kohë reale CSIRT-in kombëtar dhe atë sektorial mbi çdo zhvillim të rëndësishëm që lidhet me incidentin dhe ndajnë loget e përditësuara të trafikut për analizë të mëtejshme.

12.5 Regjistrimi

CSIRT kombëtar

a) Regjistron incidentin në platformën e menaxhimit të incidenteve, së bashku me detajet e tij.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të mbledhur informacionin e nevojshëm dhe për të siguruar që incidenti është dokumentuar plotësisht.

CSIRT sektorial

a) Aisiton CSIRT-in pranë operatorit në regjistrimin e incidentit në platformën e menaxhimit të incidenteve brenda sektorit dhe siguron që operatorët e prekur të përfshihen në këtë proces duke ndihmuar me detaje shtesë.
b) Dërgon informacionin e mbledhur drejt CSIRT-it kombëtar për të qendërzuar informacionin.

CSIRT pranë operatorit

a) Dokumenton incidentin e eksfiltrimit dhe çdo gjetje fillestare bazuar në të dhënat e mbledhura.

b) Regjistron incidentin në sistemin e menaxhimit të incidenteve sipas përcaktimeve në rregulloren e kategorizimit të incidentit të sigurisë kibernetike.
c) Raporton incidentin tek CSIRT-i kombëtar dhe ai sektorial me të gjitha detajet përkatëse.

12.6 Kategorizimi i Incidentit

CSIRT kombëtar

a) Kategorizon incidentin bazuar në natyrën dhe ndikimin e tij, si dështim i sistemit ose incident i lidhur me palë të treta apo fatkeqsi natyrore.
b) Analizon ndikimin e mundshëm të incidentit në infrastrukturën kombëtare dhe cakton një nivel të rrezikshmërisë.
c) Përditëson regjistrin e incidenteve me kategorinë e përcaktuar dhe rrezikshmërinë e incidentit.

CSIRT Sektorial

a) Asiston CSIRT-in pranë operatorit në kategorizimin e incidentit dhe komunikon atë brenda sektorit përkatës.
b) Siguron që operatorët të ndjekin procedurat e përcaktuara për menaxhimin e rrjedhjes së të dhënave.
c) Ndihmon në përcaktimin e natyrës së saktë të incidentit dhe të sistemeve të prekura.

CSIRT pranë operatorit

a) Kategorizon dhe raporton incidentin dhe siguron që të gjitha informacionet çojnë në kategorizimin e tij.
b) Vlerëson ndikimin e incidentit në proceset operacionale dhe sigurinë e të dhënave të infrastrukturës.
c) Ndjek procedurat e vendosura për menaxhimin e incidentit bazuar në kategorizimin e tij.
ç) Zbaton masa të menjëhershme për të zbutur ndikimin e rrjedhjes së të dhënave.

12.7 Prioritizimi i incidentit

CSIRT kombëtar

a) Vlerëson rëndësinë e sistemeve të prekura dhe bën prioritizimin bazuar në ndikimin e mundshëm të tij në infrastrukturën kombëtare.
b) Prioritizon përgjigjen ndaj incidentit, duke u fokusuar në ato raste ku shërbimi i ndaluar ka ndikim të lartë në reputacionin e infrastrukturës.
c) Koordinonhet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që incidentet në shërbimet më kritike të trajtohen me shpejtësi.

CSIRT Sktorial

a) Vlerëson ndikimin e aktivitetit në shërbimet kritike të sektorit dhe prioritizon sipas nevojës.
b) Koordinohet me CSIRT-in pranë operatorit për prioritizimin duke siguruar një sinkronizim të përgjigjes ndaj rrjedhjes së të dhënave.

c) Asiston CSIRT-in pranë operatorit në zbutjen e kërcënimeve më ndikimin më të lartë bazuar në vlerësimin e shërbimeve kritike.

CSIRT pranë operatorit

a) Prioritizon incidentin në bazë të ndikimit në operacionet e biznesit dhe shërbimet e klientëve.
b) Siguron burimet e nevojshme për zgjidhjen e incidentit, nisur nga ato sistene/shërbime që janë më të ndjeshme.
c) Informon CSIRT-in kombëtar dhe atë sektorial për nivelin e prioritizimit dhe përparësinë e trajtimit të incidentit.

12.8 Analiza e Incidentit

CSIRT Kombëtar

a) Analizon të gjitha të dhënat dhe raportet e mbledhura nga CSIRT-i sektorial dhe ai pranë operatorit për të kuptuar shkaqet kryesore të incidentit.
b) Bashkëpunon me partnerët ndërkombëtar për të marrë dhe aplikuar praktikat më të mira dhe eficente mbi incidentin në nivel kombëtar.

CSIRT Sektorial

a) Analizon të dhënat e siguruara nga operatorët për incidentin, duke u fokusuar në faktorët kryesorë që çuan në dështimin e sistemeve, ndalimin e shërbimeve, ose ndikimet e fatkeqësive natyrore.
b) Kontrollon për faktorë të jashtëm siç janë problemet me energjinë, temperaturën e dhomës ose dëme fizike të pajisjes.
c) Asiston operatorët në identifikimin e dobësive të proceseve operacionale dhe teknike që lejuan incidentin të ndodhë dhe analizon efektet e tij brenda sektorit.
ç) Shpërndan informacionin dhe rekomandimet analitike me operatorët e sektorit për të ndihmuar në rikthimin e shërbimeve në kohë më të shpejtë.
d) Informon CSIRT-in kombëtar për çdo zhvillim të rëndësishëm të gjetur gjatë analizimit.

CSIRT pranë operatorit

a) Analizon incidentin në nivel operativ, duke identifikuar shkakun kryesor dhe rrethanat që kanë çuar në dështimin e sistemit ose ndalimin e shërbimeve.
b) Vlerëson ndikimin mbi operacionet e përditshme dhe efektet afatgjata të incidentit, si dhe identifikon masat për zbutjen e ndikimit.
c) Shpërndan gjetjet e plota me CSIRT-in kombëtar dhe atë sektorial për ti dhënë përgjigje të sinkronizuar dhe më të shpejtë incidentit.
ç) Implementon përmirësimet e nevojshme për të parandaluar incidente të ngjashme në të ardhmen dhe përmirëson planifikimin e reagimit ndaj katastrofave.

12.9 Izolimi dhe fshirja

CSIRT Kombëtar

a) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të izoluar burimin e incidentit kryesisht në rastet kur ai vjen nga palët e treta.
b) Ofron udhëzime teknike për izolimin e sistemeve të prekur dhe mbylljen e shërbimeve të rrezikuara, duke marrë në konsideratë ndikimet mbi operacionet kombëtare.
c) Merr masa për të bllokuar çdo akses të mëtejshëm nga burimet e jashtme ose të brendshme që mund të shkaktojnë përsëritjen e incidentit.
ç) Përgatit një raport mbi masat e izolimit që duhen ndërmarr dhe e ndan atë me CSIRT-in sektorial dhe atë pranë operatorit për të ndihmuar në procesin e fshirjes dhe rikuperimit.

CSIRT Sektorial

a) Koordinon CSIRT-in pranë operatorëve me qëllim implementimin e masave të menjëhershme për izolimin e sistemeve të prekura brenda sektorit, duke ndërprerë lidhjet me palët e treta që janë bërë shkak i incidentit, deri në momentin që çështja merr zgjidhje.
b) Ofron udhëzime të detajuara për operatorët e sektorit për të kryer izolimin e duhur të pajisjeve, sistemeve dhe rrjeteve të prekur.
c) Bashkëpunon me operatorët për të identifikuar komponentët që duhet të fshihen plotësisht për të eliminuar incidentin dhe për të rivendosur operacionet në funksion normal.
ç) Shpërndan rezultatet e fazës së izolimit dhe fshirjes me CSIRT-in kombëtar për të siguruar që masat janë të koordinuara dhe të efektshme.

CSIRT pranë operatorit

a) Kryen izolimin e shpejtë të sistemeve të prekura për të parandaluar përhapjen e mëtejshme të incidentit në infrastrukturën e brendshme.
b) Ndërpret të gjitha shërbimet e prekura dhe siguron izolimin e rrjeteve të brendshme dhe pajisjeve për të shmangur rreziqe të tjera të mundshme.
c) Dokumenton çdo masë izolimi dhe fshirje të zbatuar, dhe raporton rezultatet e kësaj faze tek CSIRT-i kombëtar dhe ati sektorial për të ndihmuar në ndarjen e njohurive dhe përmirësimin e masave të sigurisë për rastet e ardhshme.

12.10 Rikthimi i shërbimeve / të dhënave

CSIRT Kombëtar

a) Ndihmon në rikthimin e çdo shërbimi të prekur nga aktiviteti i eksfiltrimit në operacione normale.
b) Koordinohet me CSIRT-in sektorial dhe atë pranë operatorit për të siguruar që të gjitha shërbimet e prekura të rikuperohen plotësisht.
c) Monitoron sistemet gjatë dhe pas rikthimit për të siguruar që aktiviteti keqdashës është zhdukur dhe për parandalimin e tij në të ardhmen.

CSIRT Sektorial

a) Ndihmon në rikthimin e shërbimeve në nivel sektorial, duke prioritizuar shërbimet ose sistmet më kritike të prekura.
b) Mbështet operatorët në rikthimin e shërbimeve në kapacitetin e plotë operacional.

c) Komunikon statusin e rikuperimit dhe çdo çështje në vazhdim drejt CSIRT-it kombëtar dhe aktorët e interesuar.

CSIRT pranë operatorit

a) Aktivizon planin e vazhdimsisë së biznesit (Business Continuity Plan).
b) Aktivizon kopjet rezervë për rikthimin e shërbimeve.
c) Verifikon integritetin dhe funksionalitetin e shërbimeve të rikuperuara përpara se të rifillojnë operacionet normale.
ç) Raporton progresin e rikuperimit dhe çdo problematikë të shfaqur gjatë rikthimit të shërbimeve drejt CSIRT-it kombëtar dhe atë sektorial për ndihmë të mëtejshme.

12.11 Aktiviteti pas incidentit

CSIRT Kombëtar

a) Harton një raport të plotë që detajon incidentin e ndodhur, veprimet e përgjigjes dhe rezultatet.
b) Rishikon aktivitetet pas incidentit për të nxjerr mësime dhe për të evidentuar fushat që kanë nevojë për përmirësim për të shmangur rastet e ngjashme.
c) Shpërndan raportin përfundimtar me CSIRT-in sektorial dhe atë pranë operatorit për të rritur gatishmërinë e përgjithshme.

CSIRT Sektorial

a) Përgatit një raport për sektorin specifik dhe përshkruan ndikimin e incidentit, veprimet e përgjigjes dhe përpjekjet e rikuperimit.
b) Asiston CSIRT-in pranë operatorit në procesin e rishikimit pas incidentit, duke kontribuar me njohuri dhe rekomandime specifike për sektorin.
c) Shpërndan mësimet e nxjerra brenda sektorit për të përmirësuar zbulimin dhe aftësitë e përgjigjes në të ardhmen.

CSIRT pranë operatorit

a) Harton raportin përfundimtar duke ofruar informacion të detajuar mbi ndikimin e incidentit, përgjigjen dhe rikuperimin.
b) Merr pjesë në procesin e mësimeve të nxjerra, duke identifikuar përmirësime operacionale dhe duke përditësuar planet e përgjigjes.
c) Zbaton rekomandimet për të forcuar mbrojtjet dhe për të përmirësuar zbulimin e ardhshëm të incidenteve të ngjashëm.