REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr.1128 prot. Tiranë, më 27.12.2024

U R DH Ë R

Nr.534 datë 27/12 / 2024

"PËR
MIRATIMIN E PLANIT KOMBËTAR PËR REAGIMIN NDAJ INCIDENTEVE TË SIGURISË KIBERNETIKE NË SHKALLË TË GJERË DHE NDAJ KRIZËS KIBERNETIKE"

Në zbatim të nenit 28, pika 8 të ligjit nr. 25/2024 "Për sigurinë kibernetike",

U R DH Ë R O J:

1. Miratimin e Planit Kombëtar për Reagimin ndaj Incidenteve të Sigurisë Kibernetike në Shkallë të Gjerë dhe ndaj Krizës Kibernetike, sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.

2. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike dhe të gjitha institucionet përgjegjëse, të cilat kanë role dhe përgjegjësi specifike të përcaktuara në Planit Kombëtar për Reagimin ndaj Incidenteve të Sigurisë Kibernetike në Shkallë të Gjerë dhe Ndaj Krizës Kibernetike, për zbatimin e këtij urdhri.

3. Ky urdhër hyn në fuqi menjëherë

DREJTOR I PËRGJITHSHËM

Igli TAFA

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

PLANI KOMBËTAR I REAGIMIT NDAJ INCIDENTEVE NË SHKALLË TË GJERË DHE KRIZËS KIBERNETIKE

Tabela e Përmbajtjes

Seksioni 1. Informacione bazë

Seksioni 1A: Situata e sigurisë kibernetike ne Shqipëri

Siguria kibernetike në Shqipëri ka marrë vëmendje të veçantë vitet e fundit, veçanërisht për shkak të sulmeve të rënda që kanë ndodhur në infrastrukturën digjitale të vendit. Shqipëria, si shumë vende të tjera, përballet me sfida të konsiderueshme në këtë fushë për shkak të digjitalizimit në rritje, mungesës së infrastrukturës së fortë mbrojtëse dhe ndërgjegjësimit të kufizuar mbi kërcënimet kibernetike.

Gjendja aktuale e sigurisë kibernetike në Shqipëri

1. Sulmet kibernetike të ndodhura
   - Në vitin 2022, Shqipëria u përball me disa sulme të rëndësishme kibernetike që u atribuan një shteti të huaj. Sulmet synuan shërbimet qeveritare dhe infrastrukturën e komunikimit elektronik.
   - Platforma si *e-Albania* dhe sisteme të tjera digjitale pësuan ndërprerje, duke ndikuar në ofrimin e shërbimeve publike.
   - Ky incident tregoi dobësitë në mbrojtjen e sistemeve kritike dhe nxiti ndërhyrje të shpejta për forcimin e sigurisë.
2. Infrastruktura dhe politikat e sigurisë kibernetike
   - Shqipëria prej vitit 2017 ka krijuar Autoritetin përgjegjës për sigurinë kibernetike. Autoriteti Kombëtar për sigurinë kibernetike bazuar në përcaktimet e ligjit nr. 25/2024 "Për sigurinë kibernetike", është institucioni përgjegjës për monitorimin dhe mbrojtjen e rrjeteve dhe sistemeve të informacionit nga sulmet kibernetike.
   - Strategjia Kombëtare për Sigurinë Kibernetike e miratuar me vendimin e Këshillit të Ministrave nr.1084, datë 24.12.2020 "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planit të Veprimit 2020-2025", synon forcimin e kapaciteteve dhe rritjen e ndërgjegjësimit.
   - Bashkëpunimi me partnerët ndërkombëtarë si NATO, Bashkimi Evropian dhe agjenci të tjera është kyç për të ngritur standardet e sigurisë kibernetike.
3. Sfida të mëdha
   - Mungesa e ekspertëve të sigurisë kibernetike: Në vend mungojnë ekspertët në fushën e sigurisë kibernetike.
   - Mungesa e ndërgjegjësimit: Individët dhe bizneset shpesh nuk i njohin kërcënimet dhe praktikat më të mira për mbrojtjen e të dhënave.
   - Mungesat në teknologji/ teknologjia e vjetër: Shumë sisteme dhe rrjete informacioni janë të mbështetura mbi infrastrukturë të vjetëruar dhe të cenueshme ndaj kërcënimeve kibernetike.
4. Masat e ndërmarra
   - Rritja e investimeve në mbrojtje kibernetike dhe teknologji të reja.
   - Modernizimi i kuadrit ligjor.
   - Monitorimi 24/7 në kohë reale i infrastrukturave të informacionit.
   - Organizimi i trajnimeve për institucionet, bizneset dhe individët.

- Parashikimi ligjor për krijimin e CERT-it, strukturë *ad-hoc* për menaxhimin dhe koordinimin e incidenteve në shkallë të gjerë dhe krizave kibernetike.
- Zbatimi i masave të sigurisë kibernetike për sektorët kritikë si energjia, financa, telekomunikacioni e të tjerë.

Roli i partnerëve ndërkombëtarë

Për shkak të anëtarësimit në NATO dhe proceseve të integrimit në BE, Shqipëria ka marrë ndihmë teknike dhe financiare për të përmirësuar sigurinë kibernetike. Partnerët ndërkombëtarë ofrojnë:

- Trajnime dhe ekspertizë për rritjen e kapaciteteve në fushën e sigurisë kibernetike.
- Teknologji dhe mbështetje financiare për të modernizuar sistemet dhe rrjetet e infrastrukturave të informacionit.

Në përmbledhje, siguria kibernetike në Shqipëri është në një fazë zhvillimi, por sfidat janë të konsiderueshme për shkak të ndërgjegjësimit të ulët dhe teknologjisë së vjetruar. Megjithatë, me mbështetjen ndërkombëtare dhe angazhimin e institucioneve vendase, vendi është në rrugën e duhur për të përmirësuar mbrojtjen nga kërcënimet kibernetike.

Hyrje dhe historik

Në vitet e fundit, me rritjen e përdorimit të teknologjive të informacionit dhe komunikimit, si dhe me avancimin e shërbimeve dhe infrastrukturave digjitale, kërcënimet ndaj sigurisë kibernetike janë bërë gjithnjë e më të pranishme dhe të sofistikuara. Ky fenomen është global dhe nuk njeh kufij, duke e bërë menaxhimin e incidenteve dhe krizave kibernetike një sfidë të rëndësishme për të gjitha shtetet. Incidentet e sigurisë kibernetike mund të përfshijnë që nga sulmet e thjeshta deri tek sulmet më të sofistikuara, si ndërprerjen e shërbimeve kritike, vjedhjen e informacionit sensitiv, apo shkatërrimin e infrastrukturave kritike dhe të rëndësishme të informacionit.

Shqipëria, si një vend anëtar i NATO-s që aspiron për t'u integruar në Bashkimin Evropian, ka bërë hapa të rëndësishëm për krijimin e një kornizë të fortë të sigurisë kibernetike, duke e konsideruar atë si një prioritet të nivelit të lartë. Në mars të vitit 2024, Shqipëria miratoi ligjin për sigurinë kibernetike, duke e përafruar pjesërisht me direktivën NIS 2, nr. 2022/2555, të Parlamentit dhe Këshillit, datë 14 dhjetor 2022, "Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, e cila ka ndryshuar rregulloren (BE) nr. 910/2014 dhe direktivën (BE) nr. 2018/1972, si dhe ka shfuqizuar direktivën (BE) nr. 2016/1148", i cili ka shënuar një hap të rëndësishëm në modernizimin e bazës ligjore me qëllim arritjen e një niveli të lartë të sigurisë kibernetike për rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë. Ky ligj është pasuar nga aktivitete të shumta për ngritjen e kapaciteteve kombëtare dhe përmirësimin e bashkëpunimit ndërmjet institucioneve të ndryshme.

Pas një rritje të ndjeshme të sulmeve kibernetike, qeveria shqiptare filloi të forcojë strukturat për menaxhimin dhe reagimin ndaj incidenteve kibernetike, duke ngritur dhe bërë funksionale Qendrën Kombëtare Operacionale të Sigurisë Kibernetike, pranë Autoritetit Kombëtar për Sigurinë Kibernetike, duke intensifikuar bashkëpunimin me NATO-n, Bashkimin Evropian dhe shtetet partnere.

Ky plan kombëtar është një instrument për të siguruar që Shqipëria të jetë e përgatitur për të përballuar çdo incident apo krizë të mundshme të sigurisë kibernetike, duke mbrojtur infrastrukturat e informacionit dhe duke siguruar vazhdimësinë e shërbimeve kyçe. Për të siguruar një menaxhim të koordinuar dhe efikas të incidenteve dhe krizave kibernetike është e rëndësishme të përfshihen të gjithë aktorët relevantë, qeverinë, sektorin privat dhe shoqërinë civile. Me anë të bashkëpunimit, koordinimit dhe trajnimit të vazhdueshëm në fushën e sigurisë kibernetike, do të bëhet e mundur që Shqipëria të përballet me sfidat e sigurisë kibernetike si dhe të reagojë në mënyrë të shpejtë dhe efikase me qëllim minimizimin e pasojave. Hartimi i këtij plani për reagimin ndaj incidenteve të sigurisë kibernetike në shkallë të gjerë dhe ndaj krizave kibernetike ka si qëllim krijimin e një kornize gjithëpërfshirëse dhe të strukturuar për identifikimin, menaxhimin dhe reagimin ndaj incidenteve dhe krizave të sigurisë kibernetike që mund të rrezikojnë funksionimin normal të shoqërisë dhe ekonomisë shqiptare.

Në këtë kuadër, ky plan synon në:

1. Koordinimin dhe bashkëpunimin ndërmjet institucioneve shtetërore, sektorit privat dhe organizatave ndërkombëtare për të krijuar një rrjet të sigurt dhe të besueshëm për menaxhimin e incidenteve kibernetike, për të ndihmuar në minimizimin e pasojave të krizave kibernetike, si dhe për të siguruar shkëmbimin e shpejtë dhe efikas të informacionit dhe të masave mbrojtëse midis shteteve, agjencive dhe aktorëve të tjerë të përfshirë në fushën e sigurisë kibernetike.
2. Përgatitjen e institucioneve dhe infrastrukturave për të reaguar ndaj kërcënimeve të sigurisë kibernetike, përfshirë masat për parandalimin e incidenteve dhe mësimet e nxjerra nga situatat e mëparshme.
3. Rritjen e kapaciteteve të reagimit dhe ndërhyrjes për të menaxhuar me sukses incidente të rëndësishme të sigurisë kibernetike dhe për të garantuar vazhdimësinë e shërbimeve dhe funksioneve shtetërore dhe private.

Rëndësia, synimet dhe objektivat e Planit Kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike

- Rëndësia e një Plani kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike

Qasja e Shqipërisë drejt digjitalizimit të shërbimeve dhe teknologjive të ndërlidhura ka rritur ndjeshëm cënueshmërinë e saj nga kërcënimet kibernetike, që variojnë nga sulmet *ransomware* mbi infrastrukturat kritike të informacionit, shkatërrim dhe marrje të të dhënave e deri te fushatat e dezinformimit. Këto kërcënime mund të ndërpresin shërbimet publike, të dëmtojnë ekonominë dhe të gërryejnë besimin e publikut. Një plan kombëtar ofron një qasje të koordinuar dhe sistematike për të adresuar këto sfida, duke siguruar që Shqipëria të jetë e përgatitur për të menaxhuar incidentet në shkallë të gjerë dhe krizat komplekse kibernetike. Një Plan kombëtar për reagimin ndaj incidenteve në shkallë të gjerë dhe krizat kibernetike është një instrument kritik për çdo shtet që synon të mbrojë infrastrukturat e veta kyçe, të garantojë sigurinë kombëtare dhe të sigurojë vazhdimësinë e shërbimeve thelbësore gjatë krizave kibernetike. Një plan i tillë siguron një kornizë për të identifikuar, analizuar dhe menaxhuar rreziqet potenciale para, gjatë dhe pas incidenteve. Plani mundëson një reagim të

koordinuar dhe efikas duke përcaktuar rolet dhe përgjegjësitë e gjithë aktorëve përfshirë, institucionet shtetërore, sektorin privat dhe aktorëve të tjerë të përfshirë në mbrojtjen kibernetike, duke shmangur konfuzionin dhe duke optimizuar reagimin në raste emergjente. Gjithashtu, plani përcakton mekanizma për të siguruar vazhdimësinë e operacioneve dhe rikuperimin e shpejtë të sistemeve pas një sulmi. Kjo është jetike për të shmangur ndërprerjet afatgjata që mund të kenë ndikime të mëdha ekonomike dhe sociale. Duke hartuar dhe miratuar këtë plan, Shqipëria demonstron angazhimin e saj për rritjen e nivelit të sigurisë kibernetike kombëtare dhe përputhjen me standardet dhe praktikat më të mira ndërkombëtare. Plani është një udhërrëfyes strategjik që synon përcaktimin e një kuadri tepër të qartë për të qenë të përgatitur për reagimin ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike.

- Synimet e Planit kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike

Plani bazohet në tre synime kryesore:

1. Parandalimi i Incidenteve dhe Reduktimi i Rreziqeve: Identifikimi proaktiv i dobësive, përmirësimi i teknikave mbrojtëse dhe minimizimi i mundësisë së krizave kibernetike.
2. Reagimi efikas ndaj Incidenteve: Krijimi i mekanizmave të fuqishëm për zbulimin, dhe zbutjen e incidenteve kibernetike për të reduktuar ndikimin e tyre në sigurinë kombëtare, ekonominë e vendit dhe qytetarët.
3. Rikuperimi dhe vazhdimësia: Aftësia për një rikuperim të shpejtë të sistemeve dhe shërbimeve të rëndësishme dhe kritike, duke siguruar vazhdimësinë e tyre pa ndërprerje.

- Objektivat e Planit kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike

Plani është strukturuar rreth tre objektivave kryesore, secili thelbësor për rritjen e nivelit të sigurisë kibernetike, mbrojtjen e sigurisë kombëtare të Shqipërisë, stabilitetit ekonomik dhe mirëqenies sociale si më poshtë vijon:

1. Ofrimi i një kornize proaktive dhe reaktive efektive ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike

Një kornizë e mirëpërcaktuar proaktive dhe reaktive efektive ndaj incidenteve është themeli i Planit kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike. Ai krijon protokolle të qarta për parapërgatitjen, zbulimin, analizimin dhe adresimin e incidenteve kibernetike në mënyrë të shpejtë dhe efikase. Kjo kornize siguron që të gjithë aktorët, institucionet shtetërore, organizatat private dhe operatorët e infrastrukturës kritike të informacionit të jenë të pajisur me mjetet, njohuritë dhe kanalet e komunikimit të nevojshme për të zbutur kërcënimet. Duke standardizuar veprimet proaktive dhe reaktive efektive, plani minimizon konfuzionin gjatë krizave dhe lehtëson një rikthim të shpejtë në normalitet.

2. Minimizimi i ndikimit të incidenteve në shkallë të gjerë dhe krizës kibernetike

Plani ka si objektiv të reduktojë dëmet e mundshme të shkaktuara nga incidentet kibernetike ndaj sigurisë kombëtare, ekonomisë dhe shoqërisë shqiptare. Sulmet kibernetike mund të

ndërpresin shërbime esenciale, të kompromet ojnë të dhënat e ndjeshme dhe të ulin besimin publik. Duke zbatuar masa proaktive, si vlerësimi i rreziqeve, monitorimi i vazhdueshëm dhe strategjitë e rikuperimit të shpejtë, plani siguron që infrastruktura dhe shërbimet kritike të mbeten funksionale edhe përballë ndërprerjeve të mëdha. Kjo qasje jo vetëm që mbron asetet digjitale të Shqipërisë, por gjithashtu forcon besimin publik në aftësinë e vendit për t'u përballur me kërcënimet kibernetike.

3. Koordinimi mes aktorëve kryesorë

Koordinimi efektiv midis institucioneve shtetërore, sektorit privat dhe partnerëve ndërkombëtarë është thelbësor për një përgjigje gjithëpërfshirëse ndaj krizave kibernetike. Plani kombëtar i reagimit ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike nxit bashkëpunimin duke përcaktuar rolet dhe përgjegjësitë, duke inkurajuar ndarjen e informacionit dhe duke shfrytëzuar ekspertizën e të gjithë aktorëve. Bashkëpunimi me organizata ndërkombëtare, si NATO dhe Bashkimi Evropian, siguron që Shqipëria të përfitojë nga praktikat më të mira globale dhe të kontribuojë në përpjekjet kolektive për sigurinë kibernetike.

Përmbledhje

1. Konteksti i vendit dhe profili i riskut

Me rritjen e përdorimit të internetit dhe digjitalizimin e shërbimeve, Shqipëria është gjithnjë e më shumë e ekspozuar ndaj kërcënimeve kibernetike. Këto kërcënime mund të vijnë nga individë, grupe kriminale, shtete ose aktorë të tjerë me qëllime të ndryshme, duke përfshirë spiunazh, sabotazh dhe vjedhje të informacionit sensitiv. Në këtë kontekst, Shqipëria ka nevojë emergjente për të siguruar një reagim të shpejtë dhe të koordinuar ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike, me qëllim sigurimin e vazhdimësisë së shërbimeve dhe mbrojtjen e infrastrukturave të informacionit dhe sigurisë kombëtare.

Sulmet kibernetike ndaj Shqipërisë arritën kulmin në vitin 2022, disa javë pas shtimit të shërbimeve online. Gjatë kësaj periudhe, Shqipëria u përball me një profil të veçantë të rrezikut kibernetikë, ku pavarësisht se disa nga shërbimet kyçe u mbyllën, vendi arriti të përballojë këto sulme të paprecedentë kibernetike, veçanërisht ato nga shteti i Iranit, duke bërë që informacioni në rrjetet dhe sistemet e tij të mbetej i sigurt.

Kërcënimet kibernetike ndodhin nga disa faktorë si:

- Pozicioni gjeostrategjik i Shqipërisë, anëtarësimi në NATO dhe bashkëpunimi ndërkombëtar e bëjnë atë një target potencial për sulme kibernetike nga shtete të tjera që synojnë të krijojnë destabilitet ose të vjedhin informacion të ndjeshëm. Ky rrezik është gjithashtu i mundshëm për shkak të ndërveprimeve të ndryshme të Shqipërisë në çështje ndërkombëtare.
- Aksesi pa limit nga punonjës në rrjete dhe sistemet e infrastrukturave të informacionit. Kërcënimet dhe incidentet kibernetike mund të vijnë gjithashtu nga aktorët e brendshëm, si punonjës që kanë akses në sistemet dhe infrastrukturat e informacionit.

- Mungesa e investimeve në infrastrukturat e informacionit, ekspozimi ndaj rreziqeve natyrore dhe katastrofave teknologjike. Këto janë faktorë të cilët mund të shkaktojnë dëme të mëdha siç janë humbje të dhënash, ndërprerje të shërbimeve dhe vështirësi në menaxhimin e krizave kibernetike.

Në këtë kontekst, Plani kombëtar për reagimin ndaj incidenteve të sigurisë kibernetike në shkallë të gjerë dhe ndaj krizave kibernetike duhet të jetë një instrument i cili adreson një gamë të gjerë kërcënimesh dhe rreziqesh që janë të pranishme në Shqipëri me fokus kryesor bashkëpunim dhe koordinim të ngushtë midis institucioneve shtetërore, sektorit privat dhe partnerëve ndërkombëtarë, me qëllim minimizimin e ndikimeve të mundshme dhe ofrimin e ndihmës së shpejtë për rikthimin dhe normalizimin e gjendjes në rastin e incidenteve në shkallë të gjerë apo krizave kibernetike.

1.1 Parimet udhëzuese të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike

1.1.1. Proaktiviteti

Parimi i proaktivitetit në reagimin ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike është një qasje thelbësore për të përballuar dhe zvogëluar ndikimin e kërcënimeve kibernetike. Ky parim përfshin veprimet parandaluese dhe përgatitjen për reagim të shpejtë përpara se incidentet të ndodhin, duke u bazuar në monitorim të vazhdueshëm, analizë të rreziqeve dhe skenarëve të mundshëm të krizës kibernetike.

Kur ndodh një krizë kibernetike në shkallë të gjerë, proaktiviteti siguron një reagim të shpejtë, të koordinuar dhe të efektshëm, duke përfshirë:

1. Identifikimin dhe izolimin e kërcënimit në kohë reale.
2. Koordinimin e të gjitha palëve të interesuara për të menaxhuar krizën (ekipe teknike, drejtues, institucionet ligjzbatuese).
3. Vlerësimin e ndikimit për të kuptuar pasojat e krizës së sigurisë kibernetike dhe prioritetin e veprimeve.
4. Rikuperimin e shpejtë të sistemeve të informacionit dhe të dhënave të kompromet uara.
5. Komunikimin e qartë publik për të siguruar transparencë dhe për të minimizuar panikun.

1.1.2. Komunikimi i qartë

Parimi i komunikimit të qartë gjatë reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike është një aspekt thelbësor për të siguruar koordinim efektiv, zgjidhje të shpejtë të problemeve dhe minimizimin e ndikimeve të krizës kibernetike. Ky parim përqendrohet në shpërndarjen e informacionit të saktë, të strukturuar dhe në kohën e duhur për të gjitha palët e përfshira.

Hapat për një komunikim efektiv gjatë krizës kibernetike janë si vijon:

1. Identifikimi i ekipit të komunikimit: Përcaktimi i personave përgjegjës për komunikimin zyrtar.

2. Përgatitja e mesazheve të gatshme për skenarë të ndryshëm krize kibernetike për të reduktuar kohën e reagimit.
3. Koordinimi i komunikimit të brendshëm dhe të jashtëm për të siguruar një mesazh konsistent.
4. Deklaratat e qarta dhe transparente që përshkruajnë situatën pa krijuar panik.
5. Monitorimi i perceptimit publik për të adresuar keqkuptimet ose informacionet e rreme.

1.1.3. Përgjegjësia dhe roli

Parimi i përgjegjësisë dhe rolit në reagimin ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike është thelbësor për të siguruar që çdo person, ekip ose entitet i përfshirë të ketë detyra dhe përgjegjësi të qarta. Ky parim siguron që reagimi ndaj incidenteve në shkallë të gjerë të jetë i organizuar, efikas dhe të shmangë vonesat ose keq-koordinimin në situata kritike. Ky parim përfshin:

1. Përcaktimin e qartë të roleve dhe përgjegjësive për individët dhe ekipet e përfshira në procesin e reagimit.
2. Krijimin e një hierarkie dhe strukture të organizuar për të mundësuar reagim të shpejtë.
3. Sigurimin që çdo palë e përfshirë e di saktësisht çfarë pritet prej saj për të përmbushur detyrat gjatë një incidenti në shkallë të gjerë dhe krize kibernetike.

1.1.4 Vlerësimi i vazhdueshëm i rrezikut

Parimi i vlerësimit të vazhdueshëm të rrezikut në reagimin ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike është thelbësor për të siguruar që infrastruktura e informacionit të ketë një kuadër të qartë të rreziqeve ekzistuese, të reja dhe në zhvillim gjatë gjithë ciklit të menaxhimit të incidentit kibernetik. Ky parim fokusohet në analizën e vazhdueshme të rreziqeve për të marrë vendime të informuara dhe për të minimizuar ndikimet e krizës kibernetike në mënyrë proaktive dhe efektive.

Vlerësimi i vazhdueshëm i rrezikut është një proces dinamik që synon:

a. Identifikimin e rreziqeve të reja dhe ekzistuese gjatë gjithë gjendjes së krizës kibernetike.
b. Analizën dhe vlerësimin e ndikimit të këtyre rreziqeve.
c. Monitorimin e vazhdueshëm për të zbuluar ndryshime në nivelin e kërcënimeve kibernetike.
ç. Marrjen e masave parandaluese dhe korrigjuese për të reduktuar efektet e incidenteve kibernetike.

1.2 Kuadri ligjor dhe rregullator

Kuadri ligjor dhe rregullator formon bazën e Planit kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike të Shqipërisë, duke ofruar udhëzime të qarta për parandalimin, menaxhimin dhe reagimin ndaj incidenteve/kërcënimeve kibernetike. Ky kuadër integron legjislacionin kombëtar, atë ndërkombëtar dhe praktikat më të mira për të siguruar një mjedis digjital të sigurt dhe të qëndrueshëm.

Duke harmonizuar legjislacionin kombëtar me *acquis* e BE-së dhe praktikat më të mira ndërkombëtare, Shqipëria demonstron angazhimin e saj për të ruajtur një ekosistem digjital të sigurt dhe të qëndrueshëm. Ky kuadër jo vetëm që adreson sfidat aktuale, por gjithashtu

pozicionon Shqipërinë për t'u përshtatur me natyrën dinamike të kërcënimeve kibernetike në të ardhmen.

Plani kombëtar i reagimit ndaj incidenteve dhe krizave kibernetike të Shqipërisë rrjedh si detyrim i ligjit nr. 25/2024 "Për sigurinë kibernetike" dhe akteve nënligjore në zbatim të tij. Ky plan ofron një kornizë strategjike referuese për reagimin ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike me qëllim sigurimin e menaxhimit efektiv të situatave të krizave kibernetike dhe mbrojtjen e infrastrukturave të informacionit dhe sigurisë kombëtare.

Përmbledhje e legjislacionit për sigurinë kibernetike në Shqipëri

Shqipëria ka zbatuar një sërë masash ligjore për të adresuar sfidat në zhvillim të sigurisë kibernetike:

Ligji nr. 25/2024 "Për sigurinë kibernetike"

- Vendos kornizën ligjore për mbrojtjen e infrastrukturave të informacionit.
- Përcakton detyrimet e subjekteve të ligjit (operatorët e infrastrukturave të informacionit) në lidhje me marrjen e masave te sigurisë me qëllim rritjen e nivelit të sigurisë kibernetike në rrjetet dhe sistemet e informacionit.
- Përcakton detyrime të qarta për operatorët e infrastrukturave të informacionit në lidhje me raportimin e detyrueshëm të incidenteve kibernetike pranë Autoritetit Kombëtar për Sigurinë Kibernetike me qëllim trajtimin në kohë të incidenteve dhe minimizimin e pasojave që ato sjellin.
- Përcakton struktura të qarta në lidhje me trajtimin e incidenteve dhe menaxhimin e krizave kibernetike, si Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike (CSIRT), në nivel Kombëtar, Sektorial dhe pranë Operatorit, Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike (CERT), Qendra Kombëtare Operacionale e Sigurisë Kibernetike (SOC).
- Përcakton subjektet e tjera përgjegjëse për sigurinë e rrjeteve dhe sistemeve të informacionit në Republikën e Shqipërisë.
- Forcon konceptin e bashkëpunimit të Autoritetit Kombëtar të Sigurisë Kibernetike më institucionet kombëtare dhe ndërkombëtar, dhe organizmave të tjerë në fushën e sigurisë kibernetike.

Ligji për Mbrojtjen e të Dhënave Personale

- Rregullon mënyrën e mbledhjes, përpunimit, ruajtjes dhe shkatërrimin e të dhënave personale.
- Përcakton masa të rrepta për të mbrojtur informacionin e ndjeshëm nga qasja e paautorizuar dhe shkeljet.

Ligji për Komunikimet Elektronike dhe Postare

- Siguron integritetin dhe sigurinë e rrjeteve dhe shërbimeve të komunikimit elektronik.
- Prezanton masa për reagimin ndaj incidenteve dhe rikuperimin nga fatkeqësitë në sektorin e telekomunikacionit.

Strategjia Kombëtare për Sigurinë Kibernetike

- Ofron një vizion strategjik për përmirësimin e qëndrueshmërisë së sigurisë kibernetike të Shqipërisë.

- Thekson ngritjen e kapaciteteve, ndarjen e inteligjencës mbi kërcënimet kibernetike dhe bashkëpunimin me partnerët ndërkombëtarë.
- Përcakton objektiva konkrete në lidhje me rritjen e nivelit të sigurisë kibernetike në rrjete dhe sisteme të informacionit në Republikën e Shqipërisë si dhe rolet dhe përgjegjësitë e institucioneve përgjegjëse për sigurinë kibernetike në vend.

Përputhshmëria me *acquis* e BE-së dhe praktikat më të mira ndërkombëtare

Kuadri ligjor në fushën e sigurisë kibernetike i Shqipërisë përputhet me *acquis* e Bashkimit Evropian dhe normat ndërkombëtare me qëllim për të siguruar konsistencë dhe ndërveprueshmëri.

Direktiva NIS 2, nr. 2022/2555, e Parlamentit dhe Këshillit, datë 14 dhjetor 2022, "Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, e cila ka ndryshuar rregulloren (BE) nr. 910/2014 dhe direktivën (BE) nr. 2018/1972, si dhe ka shfuqizuar direktivën (BE) nr. 2016/1148.

- Forcon masat e sigurisë kibernetike në shërbimet thelbësore dhe sektorët e infrastrukturës kritike të informacionit.
- Vendos standarde për menaxhimin e rrezikut dhe raportimin e incidenteve kibernetike, të cilat Shqipëria i ka integruar në legjislacionin kombëtar.

Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave Personale (GDPR), nr. 679/2016, të Parlamentit Evropian dhe të Këshillit, të datës 27 prill 2016, për mbrojtjen e personave fizikë, në lidhje me përpunimin e të dhënave personale dhe për lëvizjen e lirë të këtyre të dhënave dhe shfuqizimin e direktivës 95/46/EC.

- Legjislacioni kombëtar për mbrojtjen e të dhënave personale përputhet me kërkesat e GDPR-së, duke siguruar trajtimin e sigurt të të dhënave personale dhe përputhshmërinë me standardet e BE-së.

Konventa e Budapestit për Krimin Kibernetik

Konventa e Budapestit për Krimin Kibernetik, e miratuar nga Këshilli i Evropës në vitin 2001, është marrëveshja kryesore ndërkombëtare që synon të adresojë krimin kibernetik dhe të përmirësojë bashkëpunimin ndërkombëtar në këtë fushë. Shqipëria e ka ratifikuar këtë konventë, duke e përfshirë atë në kuadrin ligjor kombëtar për të luftuar krimin kibernetik. Pikat kryesore të Konventës dhe rëndësia e saj për Shqipërinë përfshijnë:

1. Kriminalizimin e veprimeve kibernetike

Konventa përcakton veprime që duhen konsideruar si vepra penale, duke përfshirë:

- Qasjen e paautorizuar në sisteme kompjuterike (hacking).
- Ndërprerjen e të dhënave ose shërbimeve (sulme DDoS).
- Ndërhyrjen në të dhëna (manipulimi ose fshirja e tyre).
- Prodhimin dhe shpërndarjen e malware.
- Piratimin dhe shkeljen e të drejtave të pronësisë intelektuale.
- Mashtrimet kompjuterike dhe vjedhjen e identitetit në internet.

2. Provat elektronike

- Konventa vendos rregulla për mbledhjen, ruajtjen dhe përdorimin e provave elektronike në proceset hetimore dhe gjyqësore.
- Përcakton mënyra për ruajtjen e përkohshme të të dhënave (*data preservation*), e cila është veçanërisht e rëndësishme për ndjekjen e krimeve të kryera online.

3. Bashkëpunimi ndërkombëtar
- Krijon një kornizë për bashkëpunim të shpejtë dhe efektiv ndërmjet vendeve anëtare për të hetuar dhe ndjekur krimet kibernetike.
- Përfshin shkëmbimin e informacionit, ndihmën e ndërsjellë juridike dhe ekzekutimin e kërkesave për prova ose ekstradim.

4. Roli i Shqipërisë në rajon
- Si një shtet i Ballkanit Perëndimor, Shqipëria luan një rol të rëndësishëm në bashkëpunimin rajonal për krimin kibernetik, duke përfituar nga mekanizmat e Konventës për shkëmbim informacioni dhe hetime të përbashkëta.

5. Ndërgjegjësimi dhe ndërtimi i kapaciteteve
- Përmes Konventës, Shqipëria ka akses në programe ndërkombëtare për ngritjen e kapaciteteve në luftën kundër krimit kibernetik.
- Trajnimet dhe asistenca teknike nga partnerët ndërkombëtarë ndihmojnë autoritetet shqiptare të adresojnë sfidat teknologjike.

6. Përmirësimi i sigurisë dhe besimi i publikut
- Implementimi i standardeve të Konventës ndihmon në rritjen e sigurisë së sistemeve kompjuterike dhe mbrojtjen e qytetarëve nga krimi kibernetik.
- Nxit besimin publik dhe të investitorëve në infrastrukturën digjitale të Shqipërisë.

Ratifikimi i Konventës së Budapestit dhe zbatimi efektiv i saj janë hapa të rëndësishëm për Shqipërinë në mbrojtjen e sigurisë kibernetike dhe ndjekjen penale të krimeve kibernetike në një mjedis gjithnjë e më të digjitalizuar.

1.3 Objektivat e Zhvillimit të Qëndrueshëm

Objektivat e Zhvillimit të Qëndrueshëm (OZHQ), kanë një rëndësi të madhe në fushën e menaxhimit të incidenteve në shkallë të gjerë dhe krizës kibernetike, pasi ndërlidhin aspekte sociale, ekonomike dhe teknologjike për të ndërtuar një hapësirë kibernetike më të sigurt dhe të qëndrueshme në aspektin digjital. Menaxhimi i incidenteve në shkallë të gjerë dhe krizës kibernetike lidhet veçanërisht me disa prej objektivave për të garantuar qëndrueshmëri, siguri dhe zhvillim të përgjithshëm të shoqërisë.

1**. Siguria e infrastrukturës digjitale është kyçe për zhvillimin industrial dhe inovacionin.**
- Qëllimi: Zhvillimi i infrastrukturave të informacionit të sigurta dhe elastike që mund të përballojnë sulmet kibernetike.
- Strategjitë:
  - Forcimi i sigurisë kibernetike në rrjetet dhe sistemet kritike të informacionit si: energjia, financa, uji, shëndetësia, telekomunikacioni etj.
  - Investimi në teknologji të reja për të parandaluar dhe zbuluar sulmet dhe rreziqet kibernetike.
  - Promovimi i kërkimeve shkencore për sigurinë digjitale.

2. **Siguria kibernetike është një pjesë kyçe e procesit të digjitalizimit të shërbimeve dhe komuniteteve të qëndrueshme.**
- Qëllimi: Sigurimi i sistemeve inteligjente dhe mbrojtja e të dhënave të qytetarëve në hapësirat digjitale.

- Strategjitë:
  - Krijimi i sistemeve mbrojtëse për infrastrukturat e informacionit për shërbimet digjitale.
  - Forcimi i politikave për privatësinë e të dhënave.
  - Përgatitja e shoqërisë për përballimin e krizave kibernetike përmes planeve të reagimit.

3. Edukimi me qëllim rritjen e ndërgjegjësimit dhe aftësive për të përballuar kërcënimet kibernetike.

- Qëllimi: Edukimi për sigurinë kibernetike që në faza të hershme të arsimit.
- Strategjitë:
  - Zhvillimi i programeve të trajnimit për aftësitë digjitale dhe menaxhimin e krizës kibernetike.
  - Ndërgjegjësimi i publikut për praktikat e sigurisë dhe rëndësinë e mbrojtjes së informacionit.
  - Krijimi i një kulture të sigurisë kibernetike në të gjitha nivelet e shoqërisë.

4. **Nxitja e bizneseve në investime në rrjete dhe sisteme të sigurta**

Ekonomia moderne varet nga ekosistemet digjitale që duhet të mbrohen për të siguruar rritje të qëndrueshme.

- Qëllimi: Mbrojtja e bizneseve dhe tregut të punës nga sulmet kibernetike.
- Strategjitë:
  - Rritja e investimeve në sigurinë kibernetike për mbrojtjen e bizneseve.
  - Krijimi i vendeve të reja të punës për ekspertë të sigurisë kibernetike.
  - Mbështetja e NMVM (Ndërmarrjet Mikro, të Vogla dhe të Mesme) për të zbatuar standarde të sigurisë.

5. Krijimi i politikave të qëndrueshme me qëllim rritjen e nivelit të sigurisë kibernetike në rrjetet dhe sistemet e informacionit

- Qëllimi: Zhvillimi i politikave të qëndrueshme për mbrojtjen nga sulmet kibernetike dhe promovimi i një ambienti të sigurt digjital.
- Strategjitë:
  - Krijimi i një kuadri ligjor të qëndrueshëm për sigurinë kibernetike dhe luftën kundër krimit kibernetik.
  - Forcimi i kapaciteteve të institucioneve përgjegjëse për të menaxhuar krizën kibernetike.
  - Bashkëpunimi ndërkombëtar për shkëmbimin e informacionit mbi kërcënimet globale.

6. **Bashkëpunimi ndërkombëtar në luftën kundër krizave kibernetike.**

- Qëllimi: Ndërtimi i partneriteteve ndërkombëtare për të adresuar kërcënimet kibernetike.
- Strategjitë:
  - Bashkëpunimi me organizata ndërkombëtare për shkëmbimin e njohurive dhe praktikave më të mira.
  - Ndërtimi i mekanizmave të reagimit të përbashkët ndaj krizave kibernetike.

1.4 Roli i IA në reagimin ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike

Inteligjenca Artificiale (IA) luan një rol gjithnjë e më të rëndësishëm në përballje me sfidat komplekse të sigurisë kibernetike, veçanërisht në rastet e incidenteve në shkallë të gjerë dhe krizave kibernetike. Më poshtë paraqiten disa nga mënyrat kryesore në të cilat IA kontribuon në këtë fushë:

1. Zbulimi i kërcënimeve në kohë reale
   - Analiza e sjelljes: IA përdor analiza të avancuara për të identifikuar sjelljet anormale në rrjete dhe sisteme të informacionit. Kjo përfshin monitorimin e trafikut të rrjetit dhe sjelljes së përdoruesve për të dalluar sulmet e mundshme kibernetike.
   - Identifikimi i modeleve: Algoritmet e IA mund të zbulojnë modelet dhe anomalitë që janë shumë komplekse për t'u kapur nga sistemet tradicionale të monitorimit.
2. Automatizimi i reagimit ndaj kërcënimeve kibernetike
   - Reagim i shpejtë: IA mund të marrë vendime të automatizuara për të izoluar një sistem të kompromet uar, duke parandaluar përhapjen e sulmit kibernetik.
   - Orkestrimi i reagimeve: Në rast të një krize kibernetike, IA mund të koordinojë përgjigjen midis ekipeve të ndryshme dhe sistemeve të përfshira.
3. Parashikimi dhe parandalimi
   - Modelimi i rreziqeve: IA përdor të dhëna historike dhe analiza të parashikuara për të vlerësuar dobësitë dhe për të sugjeruar masa parandaluese.
   - Mësimi i vazhdueshëm: Me çdo incident të ri kibernetik, algoritmet e IA mësojnë dhe përmirësohen për të adresuar kërcënime të ngjashme në të ardhmen.
4. Menaxhimi i krizave kibernetike
   - Përpunimi i të dhënave masive: IA mund të analizojë një volum të madh të dhënash nga burime të shumta, duke përfshirë regjistrat e sistemit, komunikimet dhe sensorët IoT, për të dhënë një pamje të plotë të situatës.
   - Vendimmarrja në kohë reale: IA mund të ndihmojë në përcaktimin e masave të sakta të reagimit duke sugjeruar zgjidhje optimale në bazë të analizave të saj.
5. Forcimi i Qendrave Operacionale të Sigurisë (SOC)
   - Zvogëlimi i alarmeve të rreme: IA mund të filtrojë dhe prioritizojë ngjarjet kibernetike për të reduktuar mbingarkesën e alarmeve të rreme.
   - Mbështetja për analistët: Ofron rekomandime dhe analiza të detajuara për ekipet e sigurisë, duke përmirësuar efikasitetin e tyre.
6. Përmirësimi i komunikimit gjatë krizave kibernetike
   - Analiza e gjuhës natyrore: IA mund të analizojë raportet, email-et dhe komunikimet e tjera për të nxjerrë informacion të rëndësishëm gjatë një incidenti kibernetik.
   - Koordinimi global: Mundëson shkëmbimin e shpejtë të informacionit ndërmjet ekipeve të shpërndara gjeografikisht.
7. Përballimi i sulmeve të avancuara dhe të përsëritura
   - Analiza e modeleve të sulmuesve: IA mund të ndihmojë në identifikimin e metodave të përdorura nga aktorët e kërcënimeve, duke krijuar profile të detajuara për kërcënimet e avancuara dhe të përsëritura.

1.5 Vlerësimi i rreziqeve dhe peizazhi i kërcënimeve kibernetike

Peizazhi digjital i Shqipërisë është gjithnjë e më i ndjeshëm ndaj një game të gjerë kërcënimesh kibernetike për shkak të adoptimit të shpejtë të teknologjisë në sektorin publik dhe atë privat. Sulmet kibernetike që synojnë infrastrukturën kritike të informacionit, sistemet e të dhënave dhe shërbimet publike janë rritur në sofistikim dhe frekuencë. Kërcënimet e zakonshme kibernetike përfshijnë:

- **Sulmet Kibernetike**: Kërcënime të vazhdueshme kibernetik, si sulmet me *Distributed Denial of Service* (DDoS) dhe fushatat phishing, që ndërpresin operacionet dhe kompromet ojnë informacionin sensitiv.
- **Dezinformimi**: Fushatat e koordinuara synojnë destabilizimin e besimit publik duke përhapur informacione të rreme, shpesh duke shënjestruar proceset politike dhe sociale.
- **Ransomware:** Sulmet me malware që enkriptojnë sistemet kritike tw informacionit dhe kërkojnë shpërblim për dekriptimin janë bërë një shqetësim i madh, veçanërisht për sektorët e shëndetësisë, financave dhe qeverisë.
- **Kërcënimet e brendshme**: Cenueshmëritë që lindin nga gabimet njerëzore ose qëllimi i keq brenda infrastrukturës së informacionit rrisin rrezikun e shkeljeve dhe humbjes së të dhënave.

Këto kërcënime që evoluojnë vazhdimisht theksojnë nevojën për një strategji të fortë të sigurisë kibernetike, të përshtatur për mjedisin gjeopolitik dhe teknologjik të Republikës së Shqipërisë.

Ndikimet e mundshme në infrastrukturën kritike të informacionit dhe shërbimet publike

Pasojat e mundshme të kërcënimeve kibernetike në infrastrukturën kritike të informacionit dhe shërbimet publike të Shqipërisë sjellin pasoja të rënda dhe me impakt të gjerë si:

- Ndërprerja e shërbimeve thelbësore: Sulmet kibernetike mund të ndërpresin rrjetet e energjisë, sistemet e ujit dhe rrjetet e komunikimit e të tjera, duke sjellë pasoja të mëdha shoqërore dhe ekonomike.
- Dëmi ekonomik: Shkeljet në institucionet financiare mund të rezultojnë në humbje të konsiderueshme financiare, ulje të besimit të publikut, investitorëve dhe pengim të rritjes ekonomike.
- Kompromet imi i të dhënave: Aksesi i paautorizuar në informacionin sensitiv mund të rrezikojë sigurinë kombëtare, besimin e publikut dhe të ekspozojë individët ndaj vjedhjes së identitetit dhe mashtrimeve.
- Ndërprerja operative: Ndërprerjet e zgjatura të shërbimeve në sektorë kritikë, si shëndetësia, transporti e të tjera, mund të kenë pasoja kërcënuese për jetën.

Natyra e ndërlidhur e këtyre infrastrukturave të informacionit amplifikon efektet zinxhir të një sulmi të vetëm, duke theksuar nevojën kritike për një menaxhim të plotë të rrezikut kibernetik.

Kategoritë e rreziqeve kibernetike

- Kërcënimet ndaj sigurisë kombëtare
  - Sulmet kibernetike ndaj sistemeve të mbrojtjes, bazave të të dhënave të inteligjencës ose mekanizmave të kontrollit kufitar mund të dobësojnë pozicionin e sigurisë së Shqipërisë.

- Operacionet kibernetike të sponsorizuara nga shteti dhe aktivitetet e spiunazhit paraqesin rreziqe të mëdha për sovranitetin dhe marrëdhëniet diplomatike të Shqipërisë.

➢ Rreziqet ekonomike
- Sulmet me ransomware dhe mashtrimet financiare ndërpresin operacionet e biznesit, duke çuar në humbje të ardhurash dhe dëmtim të reputacionit.
- Sulmet kibernetike që synojnë platformat e tregtisë elektronike dhe institucionet financiare ulin ndjeshëm besimin e konsumatorëve në shërbimet digjitale.

➢ Destabilizimi shoqëror
- Fushatat e dezinformimit manipulojnë opinionin publik, duke përkeqësuar ndarjet shoqërore dhe duke minuar proceset demokratike.
- Sulmet kibernetike ndaj shërbimeve publike mund të krijojnë panik dhe të reduktojnë besimin e shoqërisë tek qeverisja.

1.6 Organizimi i sistemit të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike

1.6.1 Hyrje

Organizimi i sistemit të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike në Shqipëri është një proces i strukturuar që synon të përmirësojë rezistencën dhe reagimin e institucioneve dhe sektorëve kritikë përballë kërcënimeve kibernetike. Ky sistem mbështetet në koordinimin ndërmjet aktorëve shtetërorë, privatë dhe ndërkombëtarë për të minimizuar ndikimet dhe për të garantuar funksionimin e vazhdueshëm të shoqërisë dhe ekonomisë.

Struktura e sistemit të reagimit ndaj incidenteve kibernetike në shkallë të gjerë dhe krizave kibernetike në Shqipëri

1. Korniza ligjore dhe strategjike

Sistemi i reagimit mbështetet në legjislacionin dhe strategjinë kombëtare për sigurinë kibernetike, të cilat përfshijnë:
- Strategjia Kombëtare për Sigurinë Kibernetike, e cila përcakton prioritetet për mbrojtjen e infrastrukturave të informacionit dhe ngritjen e kapaciteteve.
- Ligji nr. 25/2024 "Për Sigurinë Kibernetike", që përcakton:
  - ➢ Identifikimin e operatorëve kritik dhe të rëndësishëm të informacionit dhe të shërbimeve të ofruara prej tyre.
  - ➢ Detyrimin e operatorëve të infrastrukturave të informacionit për zbatimin e masave të sigurisë kibernetike për menaxhimin e riskut.
  - ➢ Detyrimet për raportimin e incidenteve të sigurisë kibernetike dhe zbatimin e masave mbrojtëse të natyrës së përgjithshme.
  - ➢ Përgjegjësitë e subjekteve të tjera përgjegjëse për sigurinë kibernetike.
- Aktet nënligjore në zbatim të ligjit nr. 25/2024 "Për Sigurinë Kibernetike" që rregullojnë:
  - ➢ Menaxhimin e incidenteve kibernetike.
  - ➢ Kategorizimin e incidenteve kibernetike.

- Identifikimin e infrastrukturave të informacionit.
- Vlerësimin dhe analizimin e nivelit të sigurisë kibernetike.
- Identifikimin, klasifikimin, përshkallëzimin dhe menaxhimin e krizës kibernetike.

- Korniza e kuadrit ligjor për mbrojtjen e të dhënave personale, e cila adreson sigurinë dhe privatësinë e të dhënave personale.

1.6.2 Kuadri i menaxhimit të incidenteve në shkallë të gjerë dhe krizës kibernetike

Kuadri i menaxhimit të incidenteve në shkallë të gjerë dhe krizës kibernetike i ofron Shqipërisë një udhërrëfyes strategjik dhe operacional për adresimin e kompleksitetit të incidenteve dhe krizës kibernetike. Ky kuadër përfshin reagimin ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike duke iu përmbajtur parimeve të koordinimit, transparencës dhe llogaridhënies, me qëllim forcimin e aftësive për të mbrojtur infrastrukturat e informacionit, ruajtur besimin e publikut dhe për të forcuar sigurinë kombëtare përballë kërcënimeve kibernetike që evoluojnë. Ky kuadër jo vetëm që adreson sfidat aktuale, por gjithashtu pozicionon Shqipërinë për t'u përshtatur me natyrën dinamike të rreziqeve të sigurisë kibernetike në të ardhmen.

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK) është institucioni përgjegjës në Shqipëri për menaxhimin e incidenteve të sigurisë kibernetike dhe koordinon veprimet me strukturat përgjegjëse në rastin e gjendjes së krizës kibernetike. Autoriteti në cilësinë e CSIRT-it Kombëtar, ofron mbështetje dhe koordinim për të gjitha institucionet dhe operatorët e infrastrukturave të informacionit në rast të incidenteve në shkallë të gjerë dhe krizës kibernetike.

1.6.3 Institucionet dhe strukturat përgjegjëse për reagimin ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike në Shqipëri

1. Struktura dhe funksionet kryesore të AKSK
   - Monitorimi dhe analiza: AKSK monitoron rrjetet dhe sistemet e informacionit për të identifikuar dhe analizuar kërcënimet dhe incidentet e mundshme kibernetike.
   - Koordinimi i reagimit: Në rast të incidenteve/krizës kibernetike, AKSK koordinon reagimin midis institucioneve të ndryshme dhe ofron udhëzime për menaxhimin e situatës.
   - Trajnimi dhe edukimi: AKSK ofron trajnime dhe aktivitete ndërgjegjësimi për të rritur kapacitetet e institucioneve dhe individëve në fushën e sigurisë kibernetike.
   - Bashkëpunimi kombëtar dhe ndërkombëtar: AKSK bashkëpunon me autoritete kombëtare dhe ndërkombëtare, organizata ndërkombëtare për të përmirësuar sigurinë kibernetike në nivel kombëtar dhe ndërkombëtar.
2. Operatorët e infrastrukturës të informacionit, kanë këto përgjegjësi:
   - Menaxhimin e rrezikut: Zbatimi i masave të sigurisë kibernetike për të mbrojtur sistemet dhe rrjetet e informacionit.
   - Raportimin e incidenteve kibernetike: Raportimi i menjëhershëm i çdo incidenti kibernetik pranë AKSK dhe CSIRT-eve sektoriale për të mundësuar një reagim të koordinuar në lidhje me menaxhimin e incidenteve kibernetike.

- Bashkëpunimi: Bashkëpunim ndërmjet AKSK dhe CSIRT-eve sektoriale me qëllim ndarjen e informacionit gjatë një incidenti në shkallë të gjerë dhe krize kibernetike.
- Plani i vazhdimësisë: Hartimi dhe aktivizimi i planeve të vazhdimësisë së veprimtarisë për të siguruar ofrimin e pandërprerë të shërbimeve gjatë një incidenti kibernetik.

3. Agjencitë e zbatimit të ligjit, kanë këto përgjegjësi:
   - Hetimi i Krimeve Kibernetike: Identifikimi dhe ndalimi i individëve ose grupeve përgjegjëse për sulmet kibernetike.
   - Analiza digjitale: Kryerja e analizave digjitale për të përcaktuar fushën dhe natyrën e incidenteve kibernetike.
   - Siguria publike: Koordinimi me agjenci të tjera për të ruajtur sigurinë dhe rendin publik gjatë një krize kibernetike.
4. Partnerët Ndërkombëtarë

   Angazhimi i Shqipërisë me partnerët ndërkombëtarë është thelbësor për adresimin e kërcënimeve kibernetike ndërkufitare. Roli i tyre përfshinë:
   - Shkëmbimi i inteligjencës: Ndarja e inteligjencës mbi kërcënimet dhe praktikat më të mira me aktorët shqiptarë të sigurisë kibernetike.
   - Mbështetje teknike: Ofrimi i ekspertizës, mjeteve dhe burimeve për të ndihmuar në menaxhimin e incidenteve komplekse kibernetike.
   - Zhvillimi i kapaciteteve: Mbështetja e Shqipërisë në forcimin e kapaciteteve të saj të sigurisë kibernetike përmes trajnimeve dhe alokimit të burimeve.
   - Koordinimi i reagimit ndaj krizave: Bashkëpunimi për përgjigje të përbashkëta ndaj krizave kibernetike që kanë implikime rajonale ose globale.

1.6.4 Subjektet përgjegjëse në menaxhimin e krizës kibernetike

Për të menaxhuar krizën kibernetike në nivel kombëtar duhet të përcaktohen rolet dhe përgjegjësitë e secilit aktor duke nisur nga nivelet më të larta drejtuese përfshirë:

1. Këshilli i Ministrave;
2. Kryeministri;
3. Komiteti Ndërministror i Sigurisë Kibernetike;
4. Ministrat;
5. Autoriteti Kombëtar i Sigurisë Kibernetike/ CSIRT Kombëtar;
6. CERT/ Ekipi i Përgjigjes ndaj Emergjencave, Krizës Kibernetike;
7. Titullari i Institucionit;
8. CSIRT Sektorial;
9. CSIRT pranë operatorit;
10. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale;
11. Policia e Shtetit.

1.6.5 Identifikimi, klasifikimi dhe hetimi i Incidentit

Identifikimi i incidentit të sigurisë kibernetike përfshin konfirmimin se një aktivitet i dyshimtë përbën një incident kibernetik. Identifikimi i incidentit kibernetik realizohet nëpërmjet analizimit të alarmeve dhe aktiviteteve të dyshimta për të përcaktuar nëse janë reale dhe të qëndrueshme.

Identifikimi i incidentit të sigurisë kibernetike 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 pranë operatorëve të infrastrukturave.
Në rastin e identifikimit të incidentit nga CSIRT-ti Kombëtar, apo nga vet operatori i infrastrukturës, struktura përkatëse në AKSK (SOC T1) dhe CSIRT-i pranë operatorit sipas kategorizimit të incidentit, me qëllim trajtimin e incidentit ekzekuton Playbook-un specifik, sipas përcaktimeve të Rregullores "Mbi procedurat e menaxhimit të incidenteve të sigurisë kibernetike, kundërmasat dhe playbooks" të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit.

Klasifikimi i incidentit të sigurisë kibernetike 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".

Analiza e incidentit të sigurisë kibernetike 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.

1.6.6 Fazat e reagimit ndaj incidenteve të sigurisë kibernetike

Fazat e reagimit ndaj incidenteve të përcaktuara në Planin Kombëtar të incidenteve në shkallë të gjerë dhe krizës kibernetike të Shqipërisë ofrojnë një qasje të strukturuar dhe efektive për menaxhimin e kërcënimeve kibernetike. Duke theksuar përgatitjen, zbulimin efikas, përgjigjen e shpejtë dhe përmirësimin e vazhdueshëm, Shqipëria forcon qëndrueshmërinë e saj ndaj incidenteve dhe krizës kibernetike. Ky kuadër proaktiv dhe gjithëpërfshirës siguron mbrojtjen e infrastrukturës të informacionit, shërbimeve publike dhe sigurisë kombëtare në një epokë gjithnjë e më digjitale.

Reagimi ndaj incidenteve të sigurisë kibernetike përfshin disa faza ku ndër më kryesoret janë:
Përgatitja e cila 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 në shkallë të gjerë.
Faza e përgatitjes përqendrohet në ndërtimin e bazave për një reagim efektiv ndaj incidenteve kibernetike duke pajisur aktorët me mjetet, kapacitetet dhe njohuritë e nevojshme. Aktivitetet kryesore përfshijnë:

- Ndërtimi i kapaciteteve: Ngritja e ekipeve të afta për reagimin ndaj incidenteve kibernetike brenda Autoritetit Kombëtar të Sigurisë Kibernetike dhe operatorëve të infrastrukturave të informacionit.
- Implementimi i teknologjive të avancuara: Vendosja e teknologjive të avancuara për monitorimin, zbulimin dhe reagimin ndaj kërcënimeve kibernetike, si sistemet *Security Information and Event Management* (SIEM) dhe mjetet për zbulimin e pikave fundore.

- Zhvillimi i politikave: Hartimi dhe përditësimi i rregullt i politikave, protokolleve dhe procedurave për menaxhimin e incidenteve dhe krizës kibernetike.
- Ndërgjegjësimi dhe trajnimi: Organizimi i sesioneve të rregullta trajnimi, simulimeve dhe fushatave të ndërgjegjësimit për të siguruar gatishmërinë në sektorët publik dhe privat.
- Rrjetet për shkëmbimin e informacionit: Ndërtimi i kanaleve të forta komunikimi midis aktorëve, përfshirë partnerët ndërkombëtarë, për ndarjen e inteligjencës dhe praktikave më të mira për kërcënimet kibernetike.

Zbulimi i incidentit kibernetik i cili përfshin proceset dhe teknologjitë për monitorimin e rrjeteve dhe sistemeve të informacionit 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.

Faza e zbulimit përfshin identifikimin dhe kuptimin e natyrës së incidentit kibernetik për të përcaktuar shtrirjen dhe ndikimin e mundshëm të tij. Hapat kryesorë përfshijnë:
- Monitorimi i kërcënimeve kibernetike: Përdorimi i mjeteve të monitorimit në kohë reale për të zbuluar anomalitë dhe aktivitetet e dyshimta brenda ekosistemit digjital.
- Identifikimi i incidenteve kibernetike: Klasifikimi i incidenteve kibernetike bazuar në rëndësinë, llojin dhe ndikimin e mundshëm, duke siguruar prioritizimin e kërcënimeve kibernetike.

Identifikimi i incidentit kibernetik i cili 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.

Komunikimi dhe koordinimi me infrastrukturat, Partnerët Ndërkombëtarë e të tjera, i cili 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 i cili 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 i cili 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 i cili 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 e cila 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.
Faza e analizës përfshin:

- Mbledhja dhe Analiza e të Dhënave: Grumbullimi i të dhënave përkatëse nga sistemet dhe rrjetet e prekura për të analizuar shkakun rrënjësor, vektorët e sulmit dhe objektivat e synuara.
- Vlerësimi i Ndikimit: Vlerësimi i pasojave të mundshme të incidentit në sigurinë kombëtare, infrastrukturën kritike dhe shërbimet publike për të udhëhequr strategjinë e reagimit.

Izolimi, fshirja dhe rikthimi i Shërbimit/ të Dhënave të cilat përfshijnë 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.
Kjo fazë përqendrohet në minimizimin e ndikimit të incidentit kibernetik, neutralizimin e kërcënimit dhe rivendosjen e sistemeve dhe shërbimeve të prekura. Veprimet kryesore përfshijnë:

- Izolimi: Zbatimi i masave për të kufizuar përhapjen e sulmit, si izolimi i sistemeve të prekura ose mbyllja e përkohshme e shërbimeve të kompromentuara.
- Eliminimi: Heqja e elementëve keqdashës nga sistemet e prekura, si malware ose pikat e paautorizuara të qasjes, duke siguruar që kërcënimi të jetë plotësisht neutralizuar.
- Rikthimi i shërbimeve: Rindërtimi ose rikthimi i sistemeve të kompromentuara duke përdorur kopje rezervë të sigurta, duke siguruar integritetin dhe funksionalitetin e tyre.
- Vazhdimësia e Shërbimeve: Aktivizimi i planeve të vazhdimësisë së biznesit për të ruajtur shërbimet thelbësore gjatë përpjekjeve të rikuperimit.
- Komunikimi me Palët e Interesuara: Ofrimi i përditësimeve të rregullta për të gjithë aktorët përkatës, përfshirë publikun, për të ruajtur transparencën dhe besimin.

Suporti për izolimin, fshirjen dhe rikthimin e Shërbimit/ të Dhënave të cilat përfshijnë asistencën që jep CSIRT-it Kombëtar për operatorët e infrastrukturave me qëllim 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 i cili 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. Kjo fazë përqendrohet në rishikimin pas incidentit me qëllim nxjerrjen e mësimeve dhe zbatimin e masave për të parandaluar përsëritjen e tij në të ardhmen. Aktivitetet kryesore përfshijnë:

- Raporti i Incidentit: Dokumentimi i detajeve të incidentit, përfshirë natyrën, ndikimin dhe masat e ndërmarra për reagimin.

- Analiza e incidentit: Kryerja e hetimeve të thelluara për të identifikuar dobësitë themelore ose çështjet sistematike.
- Përditësimi i Politikave dhe Procedurave: Rishikimi i protokolleve dhe politikave ekzistuese bazuar në mësimet e nxjerra për të përmirësuar gatishmërinë e ardhshme.
- Ndarja e informacionit me Palët e Interesuara: Angazhimi me të gjithë aktorët për të ndarë gjetjet dhe rekomandimet për përmirësim.
- Trajnimi dhe Simulimet: Integrimi i mësimeve të nxjerra në programet e trajnimit dhe simulimet e ardhshme për të testuar dhe përmirësuar strategjitë e përditësuara të reagimit.

1.6.7 Strategjitë e Komunikimit të Incidenteve dhe Krizës Kibernetike

Komunikimi efektiv është një gur themeli i Planit Kombëtar të incidenteve në shkallë të gjerë dhe krizave kibernetike në Shqipëri, duke siguruar që të gjithë aktorët të jenë të informuar dhe të përfshirë gjatë një incidenti/krize kibernetike. Komunikimi i qartë ndihmon në menaxhimin e pritshmërive publike, lehtëson koordinimin efikas dhe parandalon përhapjen e dezinformatave. Ky dokument përshkruan strategjitë për të arritur një komunikim pa ndërprerje, si brenda ashtu edhe jashtë vendit.

Strategjitë efektive të komunikimit për incidente dhe kriza kibernetike janë thelbësore për të minimizuar ndikimin dhe për të mbrojtur reputacionin e infrastrukturës. Ato ndihmojnë në sigurimin e transparencës, mbrojtjen e interesave të palëve të interesuara dhe koordinimit të përgjigjes. Disa nga aspektet kryesore të strategjive të komunikimit duhet të përfshijë:

1. **Përgatitja**

- Krijimi i një plani të komunikimit specifik për incidente kibernetike.
- Përcaktimi i ekipit të komunikimit të krizës, duke përfshirë menaxherët, ekspertët teknikë dhe zëdhënësit me median.
- Hartimi i mesazheve paraprake për skenarë të zakonshëm, si sulmet ransomware, shkeljet e të dhënave ose ndërprerjet e shërbimeve.
- Trajnimi i vazhdueshëm i stafit për të kuptuar se si duhet të reagojnë në mënyrë efektive ndaj medias dhe publikut.

2. Komunikimi

- Njoftimi i hershëm i incidenteve për palët e interesuara të brendshme dhe të jashtme.
- Sigurimi që informacioni fillestar të jetë faktik dhe i verifikuar për të shmangur konfuzionin.
- Mbajtja e një qëndrimi transparent, duke mos fshehur ndikimet potenciale.
- Shmangia e spekulimeve ose dhënies së informacionit të pasaktë.

3. Informimi i palëve në rastin e incidenteve dhe krizave kibernetike:

- Informimi i personelit: Përdorimi i komunikimit të brendshëm për të mbajtur të informuar stafin.
- Informimi i klientëve dhe partnerëve: Përdorimi i komunikimit dhe dhënia e informacionit për ndikimin mbi ta dhe hapat e ndërmarrë për t'i mbrojtur.

- Informimi i Publikut dhe media: Komunikimi dhe informimi I publikut dhe medias në lidhje me gjendjen e shkaktuar nga incidenti dhe kriza kibernetike si dhe hapat e ndërmarrë për reagimin me qëllim mbrojtjen e reputacionit të infrastrukturës.

4. **Kanale e Komunikimit duhet të përfshijnë:**
   - Kanale të brendshme: Email-i, platformat e menaxhimit të punës, mbledhje virtuale.
   - Kanale publike: Websitet zyrtare të infrastrukturave, rrjetet sociale, konferencat për shtyp.
   - Kanale të dedikuara për klientët: Helpdesku dhe shërbimi ndaj klientit për pyetje dhe shqetësime.
5. **Menaxhimi i Marrëdhënieve me Median**
   - Përgatitja e zëdhënësve për të dhënë mesazhe të qëndrueshme dhe profesionale.
   - Sigurimi që të gjitha deklaratat të jenë të sinkronizuara me ekipet teknike dhe ligjore.
   - Përdorimi i medias për të qetësuar situatën dhe për të komunikuar përparimin në zgjidhjen e incidentit dhe gjendjes së krizës kibernetike.
6. **Monitorimi dhe Përgjigja ndaj Reagimeve të publikut**
   - Monitorimi i rrjeteve sociale dhe mediave për të kuptuar perceptimin publik.
   - Përdorimi i reagimeve për të përshtatur mesazhet dhe për të adresuar shqetësimet.
   - Përgjigja e shpejtë ndaj spekulimeve ose dezinformatave që mund të qarkullojnë.
7. **Komunikimi pas incidentit/krizës kibernetike**.
   - Informimi i palëve të interesuara për veprimet parandaluese të ndërmarra pas incidentit dhe gjendjes së krizës kibernetike.
   - Raportimi i rezultateve të analizave dhe masave korrigjuese.
   - Përmirësimi i planeve të komunikimit dhe trajnimit bazuar në mësimet e nxjerra.

1.7 Modalitetet/Gjendjet e reagimit ndaj incidenteve në shkallë dhe krizave kibernetike

Aktivitetet e përshkruara në këtë Plan mbështeten në tre mënyra bashkëpunimi:

1. Modaliteti/ gjendje e përhershme
2. Modaliteti/ gjendje e paralajmërimit
3. Modaliteti/ gjendje e aktivizimit të plotë

Më poshtë paraqiten Modaliteti/ gjendjet si vijon:

1.7.1 Modaliteti i përhershëm

Modaliteti i përhershëm i referohet funksionimit normal të infrastrukturës së informacionit, gjatë së cilës bëhet ndërgjegjësimi për situatën dhe kryhen aktivitete të gatishmërisë për incidentet e sigurisë kibernetike. Komunikimet mbahen nëpërmjet raportimeve të zakonshme të incidenteve të sigurisë kibernetike sipas formateve të përcaktuara sipas kuadrit ligjor në fuqi për sigurinë kibernetike.

Identifikimi i incidenteve me shkallë të gjerë të cilët çojnë drejt situatës së krizës kibernetike bëhet nga CSIRT kombëtarë, operatorët e infrastrukturave të informacionit ,si dhe subjekte të tjera të cilat identifikojnë incidente të tilla.

1.7.2 Modaliteti i Paralajmërimit

Modaliteti i Paralajmërimit aktivizohet pas marrjes së provave dhe/ose informacionit nga infrastrukturat e informacionit apo subjektet e tjerë të prekur të cilat tregojnë për një rrezik të shtuar të një incidenti në një shkallë të gjerë në një sektor të caktuar ose sektorë të ndryshëm. Kjo mënyrë përfshin komunikimin me palët e përfshira në sektorin publik dhe sektorin privat, sipas rastit, për të forcuar shkëmbimin e informacionit dhe bashkëpunimin për të parandaluar përhapjen e mundshme të incidentit.
Gjithashtu, kjo mënyrë shërben si një filtër për të vendosur nëse është e nevojshme eskalimi/kalimi në *Mënyrën e Aktivizimit të Plotë.*

- **Aktivizimi i Mënyrës së Paralajmërimit**

Aktivizimi mund të bëhet nga CSIRT-i Kombëtar, i cili aktivizon paralajmërimin pas marrjes së një raportimi mbi identifikimin e një incidenti kibernetik i pashmangshëm të parandalohet. Gjithashtu aktivizimi mund të vijë me kërkesë edhe nga aktorë të tjerë (institucione të tjera, infrastrukturat e informacionit, subjekte që nuk janë infrastrukturë informacioni) mund të nisin gjithashtu këtë proces kur ka informacion specifik që një entitet apo sektor i tërë është në rrezik nga një incident i veçantë.
Gjatë periudhës në të cilën është në fuqi Modaliteti/ gjendja e Paralajmërimit, në të cilën janë prekura dy ose më shumë infrastruktura të informacionit angazhohen strukturat përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë plan me qëllim reagimit ndaj incidentit dhe ndarjen informacione lidhur me ecurinë e tij.
Shpërndarja e informacionit të nevojshme do të bëhet nëpërmjet kanaleve të sigurta të komunikimit duke përfshirë, shkëmbimin e informacionit, analizën, rezultatet të pajisjeve apo rrjeteve të prekura, rreziqet e mundshme të infrastrukturës dhe shërbimeve të prekura.

- **Dalja nga Modaliteti i Paralajmërimit**

Gjatë modalitetit/ gjendjes së Paralajmërimit, organizohen takime ose sesione informuese për të diskutuar procesin e vazhdueshëm të reagimit ndaj incidentit, të nevojshëm për:

- Ndalimin e përhapjes së incidentit dhe daljen nga gjendja e Paralajmërimit ose
- Eskalimin në gjendjen e Aktivizimit të Plotë.

Dy janë rezultatet e mundshme:

1. Eliminimi ose kontrollimi i rrezikut. Nëse rreziku për sektorin kritik konsiderohet se është eliminuar me sukses, zbutur ose vënë nën kontroll, atëherë gjendja e Paralajmërimit mbyllet. Veprimet e mbetura për ndjekje mund të kryhen nga vet infrastruktura, CSIRT-i Kombëtar kur kërkohet mbështetje.
2. Eskalimi në Mënyrën e Aktivizimit të Plotë. Nëse rreziqet vazhdojnë të rriten dhe nuk ka zgjidhje të parashikueshme në një afat të shkurtër, ose nëse incidenti po shkakton ose është i aftë të shkaktojë ndërprerje të rëndësishme operacionale për një sektor kritik, atëherë merret vendimi për të kaluar në fazën e aktivizimit të plotë të gjendje së krizës dhe aktivizimin e Ekipit e Përgjigjes ndaj Emergjencave dhe Krizave Kibernetike CERT-in.)

1.7.3 Modaliteti/Gjendja e aktivizimit të plotë

Kjo gjendje aktivizohet në rastet e ndodhjes se një incident që plotëson pragun e një emergjence/krize kibernetike' kombëtare, e cila kërkon aktivizimin e CSIRT+CERT pranë Autoritetit për të siguruar një strukturë efektive të koordinuar me qëllim reagimin ndërqeveritar për frenimin, zbutjen dhe/ose rimëkëmbjen.

AKSK në koordinim me strukturat e tjera përgjegjëse të sigurisë dhe mbrojtjes i paraqet Kryeministrit gjendjen e emergjencës në të cilën ndodhet vendi me qëllim propozimin për shpalljen e gjendjes së krizës kibernetike.

Vendimi për të kaluar në Modalitetin e Aktivizimit të Plotë do të merret nga Këshilli i Ministrave me propozimin e Kryeministrit. Ky vendim mund të pasojë një periudhë në të cilën Mënyra e Paralajmërimit ka qenë aktive. Megjithatë, është gjithashtu e mundur që të merret një vendim për të kaluar direkt në Aktivizimin e Plotë nëse një incident paraqitet si mjaft serioz në raportimin e parë.

- Dalja nga Modaliteti i Aktivizimit të Plotë

  Dalja nga një krizë kibernetike kërkon përmbushjen e një sërë kushtesh për të garantuar që situata është nën kontroll dhe shërbimet janë rivendosur në nivele të pranueshme. Kriteret kryesore për daljen nga një krizë kibernetike përfshijnë:
  - Rivendosja e funksionalitetit të sistemeve kritike;
  - Të gjitha sistemet e informacionit që mbështesin shërbimet kritike duhet të jenë plotësisht funksionale dhe operacionale;
  - Rilidhja prioritare e komunikimeve të rrjetit;
  - Rrjetet dhe sistemet e komunikimit të prekur duhet të rilidhen dhe të jenë të gatshme për funksionim normal, duke i dhënë përparësi shërbimeve kritike;
  - Pajisjet dhe sistemet përforcuese në gjendje pune;
  - Të gjitha përforcimet teknologjike dhe burimet shtesë të angazhuara duhet të jenë aktive dhe efektive në menaxhimin e situatës;
  - Identifikimi i shkakut rrënjësor dhe nisja e masave ndreqëse;
  - Shkaku themelor i krizës kibernetike duhet të identifikohet plotësisht dhe të jetë në proces zgjidhjeje për të parandaluar përsëritjen;
  - Konsensusi i strukturave përgjegjëse mbi arritjen e objektivave;
  - Anëtarët e strukturave përgjegjëse lidhur me reagimin ndaj situatës së emergjencës kibernetike duhet të bien dakord se objektivat për përfundimin e krizës janë përmbushur dhe se nivelet e pranueshme të shërbimeve janë rivendosur.

1.8 Aktiviteti pas incidentit

Pas përfundimit të një emergjence kibernetike, është thelbësore të analizohet dhe dokumentohet përvoja për të nxitur përmirësime të vazhdueshme. Aktivitetet kryesore pas incidentit përfshijnë:

1. Përgatitja e Raportit pas përfundimit të emergjencës/krizës kibernetike

Përvoja dhe mësimet e nxjerra nga menaxhimi i incidentit do të përfshihen në një Raport pas përfundimit të emergjencës/krizës kibernetike.

Ky raport do të përmbajë analizën e hollësishme të përgjigjes ndaj incidentit dhe do të identifikojë përmirësimet e mundshme në:

- Proceset;
- Politikat;
- Infrastrukturën teknologjike.

2. Përditësimi i Planeve dhe Udhëzimeve

- Raporti pas përfundimit të emergjencës/krizës kibernetike dhe gjetjet e tjera do të përdoren për të përditësuar Planin Kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike dhe manualët e reagimit ndaj incidenteve.
- Këto përditësime sigurojnë përmirësimin e vazhdueshëm të procesit të reagimit dhe përgatitjes për të ardhmen.

3. Ushtrime Periodike të Testimit

Këto ushtrime synojnë:

- Testimin e Planit Kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizës kibernetike si dhe planeve sektoriale të reagimit.
- Simulimin e situatave të ndryshme për të identifikuar mangësi dhe për të përmirësuar masat ekzistuese.

4. Përmirësimi i Reagimit në të gjitha nivelet

- Gjetjet nga ushtrimet dhe analizat pas incidentit do të përdoren për të forcuar:
  - Reagimin ndaj incidenteve në nivel njësie dhe sektori.
  - Koordinimin në nivel kombëtar dhe ndërkombëtar.
- Përfshirja e të gjitha palëve të interesuara siguron një përmirësim të vazhdueshëm në menaxhimin e incidenteve kibernetike.

Përfundim

Ky proces garanton një qasje sistematike për të mësuar nga përvojat, për të përmirësuar vazhdimisht planet dhe për të forcuar aftësitë e përgjigjes ndaj incidenteve kibernetike në të gjitha nivelet, duke minimizuar rrezikun e përsëritjes së krizave të ngjashme në të ardhmen.

1.9 Financimi i Sistemit të sigurisë kibernetike

Buxheti i mbrojtjes kibernetike të institucioneve sipas sektorëve të përcaktuar në anekset e ligjit nr.25/2024 “Për sigurinë kibernetike” përbehet nga:

I. Buxheti i shtetit, ku në aneksin III të ligjit nr.25/2024 “Për sigurinë kibernetike” janë detajuar efektet financiare për një afat 5-vjeçar për institucionet qendrore, institucionet rajonale, institucionet e pavarura dhe institucionet ligjzbatuese. Ky buxhet konsiston në tre shtylla kryesore ku nevojiten investime me qëllim rritjen e nivelit të sigurisë kibernetike në vend dhe më konkretisht:

- Kosto për infrastrukturën për sigurinë kibernetike (gjithë teknologjia, pajisjet harduerë, software, licencat, sistemet etj.).
- Kosto për ngritjen dhe implementimin e standardeve.
- Kostot për rritjen e kapaciteteve (trajnimet).

II. Burimet e financimit të Autoritetit Kombëtar të Sigurisë Kibernetike përbëhen nga:

- Buxheti i shtetit.
- Burime të tjera të ligjshme.

Më konkretisht në aneksin III të ligjit "Për sigurinë kibernetike" është parashikuar se AKSK duhet të parashikojë në buxhetin e 5 viteve të ardhshme nga momenti i miratimit të ligjit 40 % të buxhetit të tij vjetor për investimet në 3 shtyllat e sipërpërmendura për sigurinë kibernetike. Ndërkohë AKSHI duhet të parashikojë në buxhetin e 5 viteve të ardhshme nga momenti i miratimit të ligjit 30 % të buxhetit të tij vjetor për investimet në 3 shtyllat e sipërpërmendura për sigurinë kibernetike. Ndërsa institucionet rajonale, institucionet e pavarura dhe institucionet ligjzbatuese duhet të parashikojnë në buxhetet e 5 viteve të ardhshme nga momenti i miratimit të ligjit 30 % të buxhetit të tyre vjetor për investimet në 3 shtyllat e sipërpërmendura për sigurinë kibernetike.

1.10 Bashkëpunimi

1.10.1 Hyrje

Plani Kombëtar i reagimit të incidenteve në shkallë të gjerë dhe krizave të sigurisë kibernetike të Shqipërisë thekson rëndësinë e bashkëpunimit në të gjitha nivelet për të adresuar kompleksitetin e kërcënimeve moderne kibernetike. Përmes partneriteteve me NATO-n, BE-në, nismat rajonale dhe sektorin privat, Shqipëria ndërton një ekosistem digjital të qëndrueshëm dhe të sigurt. Këto përpjekje bashkëpunuese sigurojnë që burimet, ekspertiza dhe informacioni të mobilizohen në mënyrë efektive për të mbrojtur sigurinë kombëtare, infrastrukturën kritike dhe besimin publik.

Bashkëpunimi me partnerët kombëtarë dhe ndërkombëtarë është një komponent kritik i Planit Kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizave të sigurisë kibernetike të Shqipërisë. Në një peizazh digjital të ndërlidhur dhe globalizuar, kërcënimet kibernetike tejkalojnë kufijtë, duke kërkuar përpjekje të koordinuara midis qeverive, organizatave dhe sektorëve. Ky dokument përshkruan mekanizmat dhe strategjitë për të nxitur një bashkëpunim efektiv për të forcuar qëndrueshmërinë kibernetike të Shqipërisë.

1.10.2 Bashkëpunimi kombëtar

Bashkëpunimi kombëtar në rastet e reagimit ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike është një faktor kyç për menaxhimin e situatave të reagimit të incidenteve në shkallë të gjerë dhe krizës kibernetike. Ky bashkëpunim përfshin institucionet shtetërore, sektorin privat, institucionet arsimore dhe shoqërinë civile, duke siguruar një përgjigje të koordinuar dhe efektive ndaj incidenteve që mund të kërcënojnë sigurinë kombëtare, ekonominë dhe jetën sociale.

1.10.3 Bashkëpunimi ndërkombëtar

Bashkëpunimi ndërkombëtar në menaxhimin e incidenteve në shkallë të gjerë dhe krizave kibernetike është thelbësor për adresimin e kërcënimeve që shpesh kanë një shtrirje globale dhe prekin më shumë se një vend. Kërcënimet kibernetike janë transnacionale, dhe përballja efektive me to kërkon një qasje të koordinuar në nivel global përmes mekanizmave të bashkëpunimit, shkëmbimit të informacionit dhe reaksioneve të përbashkëta. AKSK bashkëpunon me organizmat ndërkombëtarë në fushën e sigurisë kibernetike dhe autoritetet

kombëtare të vendeve të tjera nëpërmjet marrëveshjeve të përbashkëta në përputhje me legjislacionin në fuqi për marrëveshjet ndërkombëtare.

Mekanizmat e Koordinimit me NATO-n, BE-në dhe Nismat Rajonale për Sigurinë Kibernetike

Shqipëria shfrytëzon anëtarësimet dhe partneritetet me organizata ndërkombëtare për të përmirësuar qëndrueshmërinë e saj kibernetike:

1. NATO

- Bashkëpunimi në Mbrojtjen Kibernetike: Pjesëmarrja në programet e Qendrës Bashkëpunuese për Ekselencë në Mbrojtjen Kibernetike (CCDCOE) të NATO-s për të forcuar kapacitetet mbrojtëse të Shqipërisë.
- Shkëmbimi i Inteligjencës mbi Kërcënimet: Angazhimi në platformat e NATO-s për ndarjen e inteligjencës kibernetike për të pasur akses në njohuri mbi kërcënimet në kohë reale dhe për të përmirësuar ndërgjegjësimin për situatën.
- Stërvitjet e Përbashkëta: Pjesëmarrja në stërvitjet kibernetike të udhëhequra nga NATO për të testuar dhe përmirësuar protokollet e përgjigjes.

2. Bashkimi Evropian (BE)

- Financimi dhe Mbështetja Teknike: Përdorimi i burimeve dhe mekanizmave të financimit të BE-së, si Programi Digital Europe, për ndërtimin e kapaciteteve dhe zhvillimin e infrastrukturës.
- Pjesëmarrja në Nismat e ENISA: Bashkëpunimi me Agjencinë e Bashkimit Evropian për Sigurinë Kibernetike (ENISA) për të forcuar aftësitë e zbulimit dhe reagimit ndaj kërcënimeve.
- Pjesëmarrja në Hybrid CoE për të forcuar aftësitë e zbulimit dhe reagimit ndaj kërcënimeve hibride.

3. OSBE

Bashkëpunimi i Shqipërisë me OSBE në fushën e sigurisë kibernetike konsiston në ofrimin e asistencës teknike, trajnimeve dhe promovimit të dialogut ndërkombëtar, duke mbështetur Shqipërinë në ndërtimin e një sistemi të qëndrueshëm dhe të sigurt për menaxhimin e incidenteve dhe krizave kibernetike.

4. Pjesëmarrja në forumet ndërkombëtare për Sigurinë Kibernetike

- Anëtarësimi i Shqipërisë në FIRST (Forum of Incident Response and Security Teams) me qëllim shkëmbimin e informacionit në rastet e krizave kibernetike.
- Angazhimi në Platforma Rajonale: Pjesëmarrja në forume si Forumi i Sigurisë Kibernetike i Ballkanit Perëndimor për të ndarë praktikat më të mira dhe burimet me vendet fqinje.
- Zhvillimi i Planeve të Përbashkëta për Përgjigjen ndaj Krizave: Hartimi i planeve të koordinuara me partnerët rajonalë për të adresuar kërcënimet kibernetike ndërkufitare.

1.10.4 Bashkëpunimi me sektorin privat

Sektori privat luan një rol thelbësor në ekosistemin e sigurisë kibernetike të Shqipërisë, pasi zotëron dhe operon një pjesë të konsiderueshme të infrastrukturës kritike në vend. Bashkëpunimi i ngushtë dhe efektiv me sektorin privat siguron një qasje të unifikuar për menaxhimin e incidenteve/krizave kibernetike. Ky bashkëpunim konsiston në:

1. Shkëmbimi i Inteligjencës
- Krijimi i platformave të sigurta për shkëmbimin e inteligjencës mbi kërcënimet midis institucioneve shtetërore dhe entiteteve private për të zbuluar dhe zbutur rreziqet në fazat e hershme.

2. Alokimi i Burimeve
- Lehtësimi i bashkëpunimit në vendosjen e mjeteve të avancuara për sigurinë kibernetike, si sistemet e zbulimit të kërcënimeve të bazuara në inteligjencën artificiale, për të mbrojtur si infrastrukturën publike ashtu edhe atë private.

3. Bashkëpunimi në rritjen e Kapaciteteve
- Partneriteti me drejtuesit e sektorit privat për të ofruar programe trajnimi, simulime dhe sesione për ndarjen e njohurive për ekipet e sigurisë kibernetike.

4. Bashkëpunimi për Reagimin ndaj Incidenteve
- Zhvillimi i protokolleve të përbashkëta për reagimin ndaj incidenteve për të siguruar veprime të shpejta dhe të koordinuara gjatë incidenteve kibernetike që ndikojnë si në sektorin publik dhe në atë privat.

Seksioni 2 Parandalimi/Lehtësimi

Kjo fazë përbëhet nga masa dhe procese të strukturuara që synojnë të reduktojnë mundësinë e ndodhjes së incidenteve kibernetike dhe të lehtësojnë pasojat e tyre nëse ndodhin. Ajo përfshin dy komponentë kryesorë parandalimin dhe lehtësimin të cilat përbëjnë një komponent thelbësor të një strategjie gjithëpërfshirëse për mbrojtjen dhe qëndrueshmërinë e infrastrukturave kritike dhe të shoqërisë ndaj kërcënimeve kibernetike.

2. Parandalimi

Parandalimi synon të reduktojë shanset për incidente duke përgatitur organizatat dhe duke përmirësuar sigurinë. Qëllimi kryesor i fazës së parandalimit është ulja e rrezikut të ndodhjes së incidenteve përmes masave proaktive dhe të planifikuara. Kjo përfshin:

1. Politikat dhe Strategjitë e Sigurisë Kibernetike
- Hartimi i politikave të detajuara: institucionet dhe infrastrukturat duhet të kenë politika të mirëpërcaktuara për menaxhimin e sigurisë.
- Vendosja e standardeve ndërkombëtare: Si ISO 27001 për menaxhimin e sigurisë së informacionit.

2. Vlerësimi i Rrezikut
- Identifikimi i dobësive: Vlerësimi i sistemeve kritike për të identifikuar dobësitë e mundshme teknike ose organizative.
- Monitorimi i vazhdueshëm: Implementimi i sistemeve për zbulimin e kërcënimeve në kohë reale.

3. Bashkëpunimi dhe Shkëmbimi i Informacionit

- Ndërveprimi ndërmjet institucioneve: Bashkëpunimi ndërmjet sektorëve privatë dhe publikë për ndarjen e informacionit mbi kërcënimet dhe incidentet.
- Ndërtimi i rrjeteve kombëtare dhe ndërkombëtare: Nxitja e partneriteteve për mbrojtje kibernetike.

4. Edukimi dhe Ndërgjegjësimi

- Trajnimi i stafit dhe përdoruesve: Përgatitja e personelit dhe përdoruesve për njohjen dhe menaxhimin e kërcënimeve kibernetike.
- Fushatat publike ndërgjegjësuese: Edukimi i publikut mbi praktikat e sigurta në internet.

2. Lehtësimi

Lehtësimi siguron një reagim të shpejtë dhe të efektshëm për të minimizuar ndikimin e incidenteve në shkallë të gjerë dhe krizave kibernetike. Kjo fazë fokusohet në zbutjen e ndikimit të incidenteve dhe përfshin përgjigjen e koordinuar dhe menaxhimin efektiv të krizës. Kjo fazë përfshin elementët si vijon:

1. Planifikimi i Reagimit

- Hartimi i planeve të emergjencës: Përgatitja e skenarëve të detajuar për menaxhimin e situatave të ndryshme të krizës.
- Hierarkia e vendimmarrjes: Identifikimi i roleve dhe përgjegjësive për ekipet që do të reagojnë.

2. Vendosja e Ekipeve të Specializuara

- Ekipet e reagimit ndaj incidenteve (CSIRT): Formimi i njësive të specializuara për të adresuar incidentet kibernetike.
- Ekspertët për zgjidhje teknike: Angazhimi i ekspertëve për të rikthyer sistemet në funksion sa më shpejt të jetë e mundur.

3. Strukturat e Koordinimit

- Struktura kombëtare për menaxhimin e krizës kibernetike me qëllim koordinimin e përgjigjeve në rast krize kibernetike.
- Shkëmbimi i informacionit në kohë reale: Sisteme për ndarjen dhe analizimin e informacionit ndërmjet aktorëve të ndryshëm.

4. Simulimet dhe Ushtrimet

- Testimi i planeve të reagimit: Organizimi i simulimeve për të testuar gatishmërinë e ekipeve dhe sistemeve.
- Stërvitje të rregullta: Ushtrime periodike për t'u përgatitur ndaj situatave të paparashikuara.

2.1 Rolet dhe përgjegjësitë e subjekteve përgjegjëse për sigurinë kibernetike në fazën e parandalimit

Për të menaxhuar incidentet kibernetike në nivel kombëtar duhet të përcaktohen rolet dhe përgjegjësitë e secilit aktor në fazën e parandalimit të incidentit, duke nisur nga nivelet më të larta drejtuese përfshirë:

1. Autoriteti Kombëtar i Sigurisë Kibernetike/ CSIRT Kombëtar;
2. Titullari i Institucionit;

3. CSIRT Sektorial;
4. CSIRT pranë operatorit;
5. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

1. **Autoriteti Kombëtar i Sigurisë Kibernetike**/ CSIRT Kombëtar, Ekipi i Përgjigjes ndaj Emergjencave, është Autoritet me kompetenca rregullatore, koordinuese, dhe ushtron rolet dhe përgjegjësitë e mëposhtme:

a. Harton politika të sigurisë kibernetike bazuar në standardet e mirënjohura ndërkombëtare të sigurisë si dhe aktet nënligjore në zbatim të ligjit nr.25/2024 "Për sigurinë kibernetike";
b. Krijon ekipin e përgjigjes ndaj incidenteve kibernetike/CSIRT-in Kombëtar si dhe udhëzon krijimin e ekipit të përgjigjes ndaj incidenteve kibernetike të operatorit/CSIRT pran operatorit;
c. Zhvillon trajnime në nivel kombëtar dhe ushtrime të rregullta simuluese për të siguruar një ekip të përgjigjes ndaj incidenteve kibernetike në nivel kombëtar të trajnuar dhe të gatshëm për t'ju përgjigjur incidentit, si dhe gjithashtu rishikon fazën e përgatitjes dhe dokumenton kërcënimet e reja ndërkohë që zbulohen;
ç. Zhvillon strategji të përgjigjes që prioritizojnë rreziqet bazuar në rëndësinë e ndikimit të tyre;
d. Zhvillon një plan të detajuar komunikimi për të informuar infrastrukturat, palët e interesuara dhe organet e zbatimit të ligjit rreth incidenteve kibernetike. Përcaktohen pikat e kontaktit për të gjithë anëtarët e ekipit të përgjigjes dhe sigurohet një rrjedhë komunikimi e kriptuar;
dh. Siguron si CSIRT kombëtar disponueshmërinë e mjeteve dhe zgjidhjeve të nevojshme për përgjigje ndaj incidenteve;
e. Siguron dhe udhëzon kontrollin e aksesit nëpërmjet zbatimit të masave dhe protokolleve të sigurisë me qëllim që të sigurohet vetëm aksesi i personave të autorizuar në burimet e ndjeshme.

2. **Titullari i institucionit në cilësinë e titullarit të institucionit:**
   a. Drejtojnë institucionin e tyre për koordinimin e proceseve të nevojshme në fazën e parandalimit
   b. Informojnë CSIRT-in Kombëtar në mënyrë zyrtare mbi situatën kibernetike të shërbimeve në institucionin e tyre;

3. **CSIRT Sektorial**, në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të sektorit përkatës:
   a. Siguron rritje të kapaciteteve të stafit nëpërmjet trajnimeve dhe certifikimeve periodike sipas sektorëve që mbulojnë.

4. **CSIRT pranë operatorit** në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të operatorit përkatës:
   a. Zbaton politika të sigurisë kibernetike bazuar në standardet e mirënjohura ndërkombëtare të sigurisë dhe aktet nënligjore në zbatim të ligjit nr.25/2024 "Për sigurinë kibernetike";
   b. Krijon ekipin e përgjigjes ndaj incidenteve kibernetike CSIRT pranë operatorit;

c. Siguron trajnimin dhe pjesëmarrjen në ushtrime të rregullta simuluese për të siguruar një ekip të përgjigjes ndaj incidenteve kibernetike të trajnuar dhe të gatshëm për t'ju përgjigjur incidentit, si dhe gjithashtu rishikon fazat e përgatitjes dhe dokumenton kërcënimet e reja ndërkohë që zbulohen;

ç. Zhvillon strategji të përgjigjes që prioritizojnë rreziqet bazuar në rëndësinë e ndikimit të tyre;

d. Zhvillon një plan të detajuar komunikimi për të informuar, palët e interesuara dhe organet e zbatimit të ligjit rreth incidenteve kibernetike. Përcaktohen pikat e kontaktit për të gjithë anëtarët e ekipit të përgjigjes dhe siguron një rrjedhë komunikimi e kriptuar;

dh. Siguron disponueshmërinë e mjeteve dhe zgjidhjeve të nevojshme për përgjigje ndaj incidenteve;

e. Siguron kontrollin e aksesit nëpërmjet zbatimit të masave dhe protokolleve të sigurisë me qëllim që të sigurohet vetëm aksesi i personave të autorizuar në burimet e ndjeshme.

5. **Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale** në cilësinë e institucionit përgjegjës për hartimin e politikave për mbrojtjen e të dhënave personale të individëve, monitoron zbatimin e legjislacionit përkatës në rastin e incidenteve dhe krizës kibernetike:

a. Trajton, kontrollon, dhe monitoron zbatimin e legjislacionit ne fuqi mbi mbrojtjen e te dhënave personale.

Seksioni 3: Gatishmëria

3. Gatishmëria

Të gjithë aktorët si individët dhe organizatat që mund të kontribuojnë në përpjekjet për mbrojtjen kibernetike duhet të jenë të përgatitur siç duhet. Për ta arritur këtë, është thelbësore që ata të kenë një kuptim të qartë të Planit Kombëtar për reagimin ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike, duke përfshirë rolet dhe përgjegjësitë e tyre specifike, si dhe mënyrën e integrimit të tyre në kuadrin ndërinstitucional.

Objektivi kryesor i fazës së gatishmërisë në mbrojtjen e sigurisë kibernetike dhe menaxhimin e incidenteve në shkallë të gjerë dhe krizave kibernetike është të minimizojë ndikimet negative mbi sistemet kritike, të dhënat, shëndetin, pasuritë dhe operacionet digjitale si pasojë e incidenteve kibernetike apo kërcënimeve në shkallë të gjerë. Elementët kyç të gatishmërisë përfshijnë ngritjen dhe fuqizimin e kapaciteteve për mbrojtjen e infrastrukturës kritike dhe aftësimin e institucioneve dhe organizatave për të parashikuar, për t'u përballuar dhe për t'u rimëkëmbur nga pasojat e sulmeve kibernetike apo krizave me efekt zinxhir. Kjo fazë përfshin komponentët si më poshtë:

3.1. Informimi dhe edukimi

1. Ndërgjegjësimi i Publikut:
   - Bërja e fushatave periodike informuese për të njohur kërcënimet bazë dhe mënyrat e mbrojtjes.
   - Edukimi i individëve për praktikën e mirë të përdorimit të internetit, si përdorimi i fjalëkalimeve të forta dhe identifikimi i email-eve të dyshimta.

2. Trajnimi për Profesionistët:
   - Kurse specifike për menaxhimin e incidenteve kibernetike dhe analizën e kërcënimeve.
   - Praktika dhe simulime për të përgatitur profesionistët për situata reale.
3. Politikat dhe Protokollet:
   - Hartimi dhe zbatimi i planeve të reagimit ndaj incidenteve dhe krizave kibernetike.
   - Koordinimi ndërmjet sektorëve publikë dhe privatë për një përgjigje të integruar ndaj incidenteve kibernetike.
4. Rrjetet e Bashkëpunimit:
   - Krijimi i grupeve të reagimit ndaj incidenteve kibernetike (CSIRT) për të ndarë informacion dhe për të vepruar shpejt.
   - Pjesëmarrja në iniciativa ndërkombëtare për të ndarë përvojat dhe praktikat më të mira.

3.1.1. Aktivitete të fushatave të gatishmërisë

Fushatat e gatishmërisë synojnë të ndërgjegjësojnë, edukojnë dhe përgatisin individët, organizatat dhe institucionet për të reaguar në mënyrë efektive ndaj incidenteve kibernetike dhe krizave të mëdha. Fushatat mund të realizohen në të gjithë sektorët, duke filluar nga fëmijët në shkolla, institucionet publike deri tek industria e sektorit privat. Fushata apo aktiviteti mund të modifikohet për t'iu përshtatur audiencës, por shumë prej parimeve mbeten të njëjta. Më poshtë janë disa nga aktivitetet kryesore që mund të zhvillohen:

1. Edukimi dhe Ndërgjegjësimi Publik
   - Webinare dhe Seminare: Organizimi i sesioneve online dhe fizike mbi kërcënimet kibernetike dhe praktikat më të mira për sigurinë.
   - Fushata Informative: Shpërndarja e materialeve edukative (broshura, postera, video) përmes mediave sociale, televizionit dhe platformave të tjera mediatike.
   - Dita Kombëtare e Sigurisë Kibernetike: Vendosja e një dite të dedikuar për ndërgjegjësimin për sigurinë kibernetike, me aktivitete publike si demonstrime dhe leksione të hapura.
2. Trajnime dhe Simulime
   - Trajnime për Stafin Teknik dhe Drejtuesit: Ofrohen kurse për stafin e organizatave publike dhe private mbi menaxhimin e incidenteve dhe përdorimin e mjeteve të avancuara për identifikimin e kërcënimeve.
   - Simulime të Incidenteve: Kryerja e stërvitjeve për të testuar reagimin e ekipeve ndaj sulmeve të simuluara, si sulmet DDoS, ransomware ose ndërhyrjet në sisteme.
   - Ushtrime Kombëtare dhe Rajonale: Organizimi i ushtrimeve të koordinuara ndërinstitucionale për të përmirësuar bashkëpunimin në rast krize.
3. Krijimi i Infrastrukturës së Informimit dhe Mbështetjes
   - Platforma për Ndërgjegjësim: Zhvillimi i faqeve të internetit ose aplikacioneve që ofrojnë udhëzime të qarta për raportimin dhe menaxhimin e incidenteve kibernetike.
   - Qendrat e Ndihmës: Vendosja e linjave telefonike dhe qendrave të ndihmës për të mbështetur qytetarët dhe bizneset gjatë incidenteve.

- Sisteme të Paralajmërimit të Hershëm: Implementimi i mekanizmave për paralajmërimin e hershëm të kërcënimeve të reja kibernetike.

4. Ndarja e Informacionit dhe Bashkëpunimi Ndërinstitucional
   - Rrjetet e Bashkëpunimit: Krijimi i grupeve të reagimit ndaj incidenteve kibernetike (CSIRT) për të ndarë informacion dhe burime.
   - Partneritete Publike-Private: Promovimi i bashkëpunimit ndërmjet sektorëve publikë dhe privatë për të rritur aftësinë kolektive të reagimit.
   - Workshop-e Ndërkombëtare: Organizimi i takimeve me organizata ndërkombëtare për shkëmbimin e praktikave më të mira dhe standardeve.
5. Mbështetja dhe Promovimi i Teknologjive të Sigurisë
   - Testimi dhe Përmirësimi i Sistemeve: Inkurajimi i organizatave për të testuar dobësitë në infrastrukturat e tyre dhe për të implementuar masa të reja mbrojtëse.
   - Adoptimi i Teknologjive të Reja: Promovimi i përdorimit të teknologjive si inteligjenca artificiale dhe blockchain për të përmirësuar sigurinë dhe mbrojtjen.
   - Grante për Siguri Kibernetike: Sigurimi i fondeve për bizneset dhe institucionet që investojnë në siguri kibernetike.
6. Përhapja e Kulturës së Sigurisë Kibernetike
   - Fushata të Brendshme: Organizimi i aktiviteteve për rritjen e ndërgjegjësimit të stafit për sulmet si phishing dhe inxhinieria sociale.
   - Angazhimi i Komunitetit të IT-së: Përfshirja e komuniteteve të zhvilluesve dhe ekspertëve për të ndihmuar në identifikimin dhe parandalimin e kërcënimeve.
   - Programet Edukative për Fëmijët dhe Nxënësit: Edukimi i brezit të ri mbi sigurinë kibernetike përmes kurseve dhe aktiviteteve shkollore.
7. Vlerësimi dhe Përmirësimi i Planeve të Gatishmërisë
   - Auditime të Sigurisë: Kryerja e auditimeve të rregullta për të identifikuar dobësitë në sistemet dhe procedurat ekzistuese.
   - Përmirësimi Bazuar në Përvojë: Analiza e të dhënave dhe rezultateve nga simulimet dhe incidentet për të rregulluar dhe përmirësuar planet e reagimit.
   - Raporte për Ndikimin: Publikimi i raporteve periodike për të rritur ndërgjegjësimin dhe transparencën mbi rreziqet dhe masat e marra.

3.2 Paralajmërimi i hershëm

Paralajmërimi i hershëm është një komponent thelbësor në menaxhimin e incidenteve dhe krizave kibernetike, që synon të identifikojë dhe të komunikojë rreziqet potenciale në kohë, për të minimizuar ndikimet negative mbi sistemet kritike dhe shoqërinë në përgjithësi.
Qëllimi i paralajmërimit të hershëm është:

1. Parashikimi i kërcënimeve kibernetike: Identifikimi i shenjave të hershme të sulmeve të mundshme, si aktivitete të pazakonta në rrjete ose lëshimi i malware të ri.
2. Përgatitja e aktorëve përkatës: Informimi i infrastrukturave dhe individëve për të marrë masa parandaluese dhe për t'u përgatitur për një përgjigje efektive.
3. Reduktimi i dëmeve: Parandalimi i përhapjes së ndikimit të sulmeve duke reaguar në kohë dhe duke përmirësuar mbrojtjen para se të ndodhë një incident i madh.

Komponentët kryesor të procesit të paralajmërimit të hershëm janë:

1. Zbulimi i kërcënimit: Identifikimi i aktiviteteve të dyshimta ose shenjave të hershme për një sulm të mundshëm kibernetik.
2. Vlerësimi i ndikimit: Analiza e potencialit të rrezikut dhe vlerësimi i ndikimit të mundshëm mbi sistemet kritike dhe organizatat.
3. Komunikimi i paralajmërimit: Dërgimi i informacionit tek aktorët përkatës përmes kanaleve të sigurta dhe të strukturuara.
4. Aktivizimi i masave parandaluese: Zbatimi i masave teknike dhe organizative, si përditësimet e sigurisë dhe aktivizimi i planeve të emergjencës.

3.2.1. Sistemet e vëzhgimit, monitorimit dhe parashikimit

Monitorimi sistematik i rreziqeve që vijnë si rezultat i kërcënimeve kibernetike, kërkon përcaktimin e saktë të roleve dhe të përgjegjësive të institucioneve dhe strukturave monitoruese dhe informuese/njoftuese dhe atyre të mbrojtjes. Gjithashtu, kërkohet vendosja e linjave të qarta të komunikimit, informimit dhe raportimit midis strukturave monitoruese dhe informuese/njoftuese të mbrojtjes.

Sistemet e vëzhgimit, monitorimit dhe parashikimit luajnë një rol thelbësor në adresimin e incidenteve në shkallë të gjerë dhe krizave kibernetike. Këto sisteme janë të dizenjuara për të identifikuar, analizuar dhe reaguar ndaj kërcënimeve kibernetike, duke ndihmuar infrastrukturat të minimizojnë ndikimin dhe të rikuperohen shpejt. Këto sisteme dhe strategji janë të domosdoshme për një qasje proaktive dhe të qëndrueshme ndaj sigurisë kibernetike, duke minimizuar rreziqet dhe duke rritur rezistencën ndaj krizave.

Procedura e monitorimit kryhet nga strukturat përkatëse pranë CSIRT-it Kombëtar si dhe nga ato pranë operatorit me qëllim zbulimin dhe reagimin ndaj sulmeve apo incidenteve të mundshme kibernetike mbi rrjetet dhe sistemet e informacionit.

CSIRT-it Kombëtar në kuadër të aktivitetit monitorues në rastet e identifikimit të kërcënimeve kibernetike paralajmëron, njofton dhe shpërndan informacion pranë infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe subjekteve përgjegjëse në lidhje me rreziqet e mundshme, vulnerabilitetet dhe incidentet kibernetike.

3.3 Trajnimi dhe Ndërtimi i Kapaciteteve

3.3.1 Trajnimi dhe Ndërtimi i Kapaciteteve

Suksesi i Planit Kombëtar të reagimit ndaj incidenteve dhe krizave të sigurisë kibernetike varet nga disponueshmëria e profesionistëve të aftë dhe një sektor publik dhe privat të mirë-informuar. Iniciativat efektive të trajnimit dhe ndërtimit të kapaciteteve janë thelbësore për të zhvilluar ekspertizën e nevojshme për të adresuar kërcënimet kibernetike dhe për të nxitur një kulturë ndërgjegjësimi për sigurinë kibernetike në të gjitha nivelet e shoqërisë.

Trajnimi dhe zhvillimi janë koncepte tejet të gjera dhe një nga aspektet më të rëndësishme për t'u marrë në konsideratë janë specifikat e tyre. Trajnimi mund të realizohet në nivel personal, profesional dhe akademik, si dhe në ekipe, në nivel sektori, institucional apo organizate. Trajnimi dhe zhvillimi në partneritet inkurajohet fort dhe zakonisht është efikas nga pikëpamja

e kostos. Kur merret në konsideratë një plan disavjeçar i trajnimeve dhe ushtrimeve, duhet të identifikohet një institucion i qartë përgjegjës, i cili për Shqipërinë do të jetë AKSK-ja.

Plani disavjeçar i trajnimeve dhe ushtrimeve është një dokument strategjik dhe udhëzues që zbatohet nga Autoriteti Kombëtar i Sigurisë Kibernetike (AKSK). Si një dokument dinamik, ai është subjekt përditësimesh dhe përmirësimesh të rregullta çdo vit, për të reflektuar zhvillimet e reja në fushën e sigurisë kibernetike.

Ky plan ofron një udhërrëfyes të detajuar për AKSK-në, infrastrukturat e informacionit, dhe institucionet publike dhe private, duke përcaktuar aftësitë kryesore që duhen zhvilluar. Ai lidhet ngushtë me prioritetet kombëtare dhe përmban trajnimet dhe ushtrimet e nevojshme për t'i përftuar ose validuar këto aftësi.

Plani gjithashtu përfshin një model të detajuar të kalendarit të trajnimeve dhe ushtrimeve, i cili përshkruan aktivitetet e propozuara për periudhën e planifikuar. Ky model synon të sigurojë një qasje të organizuar dhe të koordinuar për ngritjen e kapaciteteve në reagimin ndaj incidenteve dhe krizave kibernetike.

3.3.2 Zhvillimi i Aftësive për Profesionistët e Sigurisë Kibernetike

Ndërtimi i një grupi të fuqishëm profesionistësh në sigurinë kibernetike është jetik për qëndrueshmërinë e Shqipërisë ndaj kërcënimeve kibernetike. Iniciativat kryesore përfshijnë:

1. Programet e Trajnimit të Specializuar
   - Krijimi dhe zgjerimi i programeve të trajnimit për profesionistët e sigurisë kibernetike, me fokus në zbulimin e kërcënimeve kibernetike, reagimin ndaj incidenteve kibernetike dhe menaxhimin e rreziqeve të sigurisë kibernetike.
   - Bashkëpunimi me institucionet akademike për të ofruar kurse të specializuara dhe certifikime në sigurinë kibernetike.
2. Rritja e Kapaciteteve për Ekipet e Reagimit ndaj Incidenteve
   - Pajisja e ekipeve kombëtare të reagimit ndaj incidenteve kibernetike me mjetet dhe teknikat më të fundit për të menaxhuar krizat komplekse të sigurisë kibernetike.
   - Organizimi i ushtrimeve dhe simulimeve të rregullta për të testuar dhe përmirësuar aftësitë teknike të ekipeve të reagimit ndaj incidenteve të sigurisë kibernetike.
3. Bashkëpunimi Ndërkombëtar
   - Partneritet me NATO-n, BE-në dhe organizata të tjera ndërkombëtare për të lehtësuar shkëmbimin e njohurive dhe ofrimin e mundësive të trajnimit në fushën e sigurisë kibernetike.
   - Inkurajimi i pjesëmarrjes në forume ndërkombëtare për çështje të sigurisë kibernetike.
4. Zhvillimi i Vazhdimësisë Profesionale
   - Zbatimi i nismave për të nxitur mësimin e vazhdueshëm për të mbajtur profesionistët të përditësuar mbi kërcënimet dhe teknologjitë që po shfaqen.
   - Sigurimi i aksesit në burime online, platforma trajnimi dhe rrjete ekspertësh me qëllim mbajtjen e përditësuar të ekspertëve të sigurisë kibernetike.
5. Rritja e Ndërgjegjësimit në Sektorët Publik dhe Privat

Siguria kibernetike është një përgjegjësi e përbashkët që kërkon pjesëmarrje aktive nga institucionet publike dhe entitetet private.

3.3.3 Strategjitë kryesore në kuadër të trajnimeve dhe zhvillimit të kapaciteteve përfshijnë:

1. Fushatat e Ndërgjegjësimit Publik
   - Nisja e fushatave kombëtare për të edukuar qytetarët mbi praktikat bazë të sigurisë kibernetike, si njohja e përpjekjeve phishing dhe sigurimi i pajisjeve personale.
   - Zhvillimi i materialeve si broshura, video dhe faqe interneti për të shpërndarë këshilla dhe udhëzime për sigurinë kibernetike.
2. Trajnimi i Përshtatur për Sektorin
   - Organizimi i vazhdueshëm i sesioneve trajnuese të përshtatura për sektorët kyç, përfshirë energjinë, financat, shëndetësinë dhe telekomunikacionet, për të adresuar rreziqet e sigurisë kibernetike, menaxhimi i incidenteve dhe krizave të sigurisë kibernetike.
   - Sigurimi i trajnimeve për nivelin ekzekutiv për drejtuesit në qeveri dhe organizata private për të theksuar rëndësinë strategjike të sigurisë kibernetike.
3. Bashkëpunimi Publik-Privat
   - Nxitja e partneriteteve midis agjencive qeveritare dhe kompanive private për të ndarë njohuri, mjete dhe praktika më të mira në fushën e sigurisë kibernetike.
   - Inkurajimi i organizatave private për të miratuar dhe promovuar masa të forta të sigurisë kibernetike mes punonjësve dhe aktorëve të tjerë.
4. Integrimi në Edukim
   - Futja e temave të sigurisë kibernetike në kurrikulën shkollore për të kultivuar ndërgjegjësimin e hershëm mes nxënësve.
   - Mbështetja e programeve jashtëshkollore si klubet e kodimit dhe garat e sigurisë kibernetike për të frymëzuar profesionistët e ardhshëm.

Përfundim

Trajnimi dhe ndërtimi i kapaciteteve janë pjesë përbërëse të Planit Kombëtar të incidenteve në shkallë të gjerë dhe krizave të sigurisë kibernetike. Duke pajisur profesionistët me aftësi të avancuara dhe duke nxitur ndërgjegjësimin në sektorët publik dhe privat, Shqipëria forcon aftësinë e saj për të parashikuar, parandaluar dhe reaguar ndaj kërcënimeve kibernetike duke siguruar qëndrueshmërinë e vendit në një botë gjithnjë e më digjitale, si dhe duke ndërtuar një kulturë përgjegjësie dhe vigjilence të përbashkët.

3.3.3 Koordinimi

AKSK në përputhje me parashikimet e ligjit nr. 25/2024 “Për sigurinë kibernetike”, me urdhër të drejtorit të përgjithshëm dhe në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, zhvillon dhe nxit, sa herë vlerësohet e nevojshme, trajnime për personelin e këtyre operatorëve, në kuadër të përmbushjes me efektivitet të lartë të detyrave.

Gjithashtu Bazuar në Strategjinë Kombëtare për Sigurinë Kibernetike 2020-2025 [1]është parashikuar si një ndër objektivat kryesor rritja e ndërgjegjësimit dhe e aftësive profesionale të institucioneve publike dhe private për sigurinë kibernetike, e cila përfshin:

- Trajnime periodike për thellimin e njohurive në sigurinë kibernetike, sipas dinamikës së fushës, për stafin administrativ në nivel qendror dhe në nivel lokal.
- Rritja dhe mbështetja e kapaciteteve kërkimore dhe risive të biznesit nëpërmjet nxitjes së ngritjes së qendrave kërkimore shkencore në fushën e sigurisë kibernetike.
- Rritja e kapaciteteve të CSIRT-eve në nivel kombëtar dhe nivelit ekzekutiv të administratës publike nëpërmjet trajnimeve dhe stërvitjeve kibernetike.
- Rritje e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe për kërcënimet kibernetike.

3.3.4 Cikli i zhvillimit

Cikli i zhvillimit bazuar në statusin aktual të AKSK-së dhe të partnerëve të saj strategjikë, Plani Disavjeçar i Trajnimeve dhe Ushtrimeve duhet të zhvillohet nga ana funksionale dhe të bazohet në objektiva specifikë, të matshëm, të arritshëm, realistë dhe të bazuara në kohë ose sipas tipit të tyre. Evidencat janë marrë nga dokumenti Raporti Kombëtar i Vlerësimit të Riskut të Sigurisë Kibernetike. Njohja është elementi kyç në koordinimin e treguesve bazë të kapacitetit dhe aftësisë së strukturave operacionale dhe të institucioneve dhe strukturave të mbrojtjes civile.

3.3.5 Testimi dhe Ushtrimet e Simulimit

Testimi dhe ushtrimet e simulimit janë përbërës thelbësorë të Planit Kombëtar të incidenteve në shkallë të gjerë dhe krizave të sigurisë kibernetike. Këto aktivitete sigurojnë që masat e sigurisë kibernetike të vendit të jenë efektive, të përshtatshme dhe të mirë-koordinuara. Duke riprodhuar kërcënimet kibernetike reale, aktorët mund të identifikojnë dobësitë, të përmirësojnë bashkëpunimin dhe të rrisin gatishmërinë e përgjithshme në mbrojtjen ndaj tyre. Ushtrimet e testimit dhe simulimit janë jetike për të siguruar efektivitetin e Planit Kombëtar të Incidenteve në shkallë të gjerë dhe krizave të sigurisë kibernetike. Duke vlerësuar rregullisht protokollet e reagimit, duke forcuar koordinimin dhe duke u përshtatur me kërcënimet që evoluojnë, këto ushtrime rrisin gatishmërinë dhe qëndrueshmërinë e Shqipërisë për përballimin e incidenteve kibernetike në shkallë të gjerë dhe krizave kibernetike. Angazhimi për përmirësim të vazhdueshëm përmes testimit thekson qasjen proaktive të vendit për të mbrojtur ekosistemin e tij digjital.

Rëndësia e Ushtrimeve dhe Simulimeve të Rregullta konsiston në:

1. **Protokollet të Reagimit**
   - Ushtrimet ndihmojnë në testimin praktik të protokolleve të reagimit, duke siguruar që ato të jenë efektive dhe të përshtatura me skenarët realë.
   - Simulimet zbulojnë boshllëqet në gatishmëri, duke ofruar mundësi për përmirësim.
2. **Përmirësimi i Koordinimit të Aktorëve**

[1] Miratuar me Vendimin e Këshillit të Ministrave nr. 1084, datë 24.12.2020, "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planit të veprimit 2020-2025".

- Ushtrimet e rregullta nxisin bashkëpunimin midis agjencive qeveritare, entiteteve të sektorit privat dhe partnerëve ndërkombëtarë.
- Sigurojnë që të gjithë aktorët të kuptojnë rolet dhe përgjegjësitë e tyre në një situatë krize kibernetike.

3. **Ndërtimi i Besimit**

- Trajnimi në kushte të simuluara ndërton besim midis ekipeve të sigurisë kibernetike dhe strukturave vendimmarrësve.
- Forcon besimin e sektorit publik dhe privat në aftësinë e Shqipërisë për të menaxhuar incidente komplekse kibernetike dhe për të përballuar situatat e krizave kibernetike.

4. Përshtatshmëria me Kërcënimet Kibernetike

- Kërcënimet kibernetike janë vazhdimisht në ndryshim, simulimet ndihmojnë në testimin e taktikave dhe teknologjive të reja për të adresuar rreziqet e reja.

3.3.5.1 Ushtrimet në tavolinë (*Table Top Exercise* - TTX)

Ushtrimet simuluese në sigurinë kibernetike përfshijnë pjesëtarë të stafit të nivelit të lartë, nëpunës të zgjedhur apo të emëruar dhe personel nga sektorë të ndryshëm. Këto ushtrime kanë si qëllim diskutimin e skenarëve të simuluar të kërcënimeve dhe incidenteve kibernetike, ose për të vlerësuar llojet e sistemeve të nevojshme për të drejtuar parandalimin, përgjigjen dhe rimëkëmbjen nga një emergjencë e caktuar kibernetike.

Ky lloj ushtrimi synon të:

- Nxisë diskutime strategjike dhe operacionale mbi çështje të ndryshme që lidhen me një situatë hipotetike kibernetike, si sulmet DDoS, ransomware, apo kompromentimet e infrastrukturës kritike.
- Vlerësojë planet, politikat dhe procedurat e sigurisë kibernetike për të identifikuar pikat e forta dhe dobësitë.
- Testojë sistemet e vendimmarrjes dhe koordinimit, duke përgatitur pjesëmarrësit për parandalimin, reagimin dhe rimëkëmbjen nga sulmet kibernetike.

Objektivat e Ushtrimeve Simuluese për Sigurinë Kibernetike

- Lehtësimi i të kuptuarit të koncepteve: Përmes diskutimeve të thelluara, pjesëmarrësit fitojnë një kuptim më të mirë të kërcënimeve kibernetike dhe masave mbrojtëse.
- Zhvillimi i aftësive për vendimmarrje: Në një ambient të kontrolluar dhe me ritëm të qetë, pjesëmarrësit praktikojnë zgjidhjen e problemeve komplekse kibernetike pa presionin e një emergjence reale.
- Përmirësimi i politikave dhe procedurave: Rekomandimet nga diskutimet ndihmojnë në rishikimin dhe përditësimin e strategjive ekzistuese.

Përfitimet dhe Kosto-Efikasiteti i Ushtrimeve Simuluese

Ndryshe nga ushtrimet e bazuara në operacione dhe lojërat e ndërlikuara, ushtrimet simuluese në tavolinë (TTX) janë mjete efektive nga pikëpamja e kostos dhe mund të përdoren së bashku me ushtrime më komplekse. Përdorimi i tyre në kontekstin e sigurisë kibernetike përfshin:

- **Diskutime të thelluara**: Pjesëmarrësit inkurajohen të analizojnë skenarë kibernetikë në detaje dhe të ofrojnë zgjidhje.

- **Zbatimi gradual i përmirësimeve**: TTX-të lejojnë ndryshimin dhe përshtatjen e politikave dhe procedurave në një mjedis të qetë dhe të strukturuar.
- **Ndërtimi i një kulture sigurie**: Pjesëmarrësit përvetësojnë koncepte dhe qasje të reja që ndihmojnë në përmirësimin e gatishmërisë ndaj incidenteve kibernetike.

Ushtrimet simuluese për sigurinë kibernetike janë një instrument i domosdoshëm për testimin dhe përmirësimin e kapaciteteve kombëtare dhe institucionale, duke kontribuar në forcimin e gatishmërisë dhe mbrojtjes ndaj incidenteve kibernetike.

3.3.5.2 Simulime Praktike (Live-Action Simulations)

Simulimet praktike, të njohura edhe si *Live-Action Simulations,* janë ushtrime realiste që testojnë aftësitë teknike, operacionale dhe strategjike të një organizate për të parandaluar, zbuluar, reaguar dhe rimëkëmbur nga incidente kibernetike. Në këto simulime, krijohen kushte sa më të afërta me situatat reale për të vlerësuar në mënyrë gjithëpërfshirëse kapacitetet dhe dobësitë në një mjedis të kontrolluar.

Simulimet praktike janë një nga mjetet më efektive për të testuar dhe forcuar mbrojtjen kibernetike të një infrastrukture. Ato ndihmojnë në vlerësimin e gatishmërisë teknike dhe organizative ndaj incidenteve të ndërlikuara, duke ofruar një pasqyrë të qartë të përmirësimeve të nevojshme. Megjithëse kërkojnë burime të konsiderueshme, përfitimet afatgjata i tejkalojnë kostot, duke ndihmuar infrastrukturat të mbrohen më mirë nga sfidat në një mjedis gjithnjë e më të ndërlikuar kibernetik.

3.3.5.3 Ushtrime të Përshtatura për Sektorë të Veçantë

Ushtrimet e përshtatura për sektorë të veçantë janë një metodë e fokusuar për të testuar dhe përmirësuar aftësitë e sigurisë kibernetike, duke marrë parasysh kërkesat specifike, kërcënimet dhe rregulloret që lidhen me sektorët e ndryshëm. Këto ushtrime janë të dizenjuara për të trajtuar sfidat unike të çdo sektori, duke siguruar që infrastrukturat të jenë të përgatitura për të menaxhuar rreziqet kibernetike në mjedisin e tyre specifik.

- **Përshkrimi:** Simulime të përshtatura për sektorë kritikë, përfshirë energjinë, financat, shëndetësinë dhe telekomunikacionet.
- **Frekuenca:** Zhvillohen dy herë në vit, duke u fokusuar në dobësitë specifike të sektorëve dhe mekanizmat e reagimit.
- **Objektivat:** Forcimi i qëndrueshmërisë së sektorëve dhe integrimi i planeve të sektorëve specifikë me kuadrin kombëtar.

3.3.5.4 Stërvitjet e Specialitetit (Drills) në Sigurinë Kibernetike

Stërvitjet e specialitetit në sigurinë kibernetike janë aktivitete të strukturuara dhe të mbikëqyrura që kanë për qëllim testimin dhe përmirësimin e një funksioni specifik ose një operacioni të veçantë brenda një organizate. Ato janë të dizajnuara për të siguruar trajnim të përqendruar dhe për të testuar në mënyrë të detajuar kapacitetet teknike dhe operacionale, duke ndihmuar organizatat të përmirësojnë reagimin dhe aftësitë në menaxhimin e incidenteve kibernetike.

Përdorimi dhe Qëllimi i Stërvitjeve të Specialitetit

1. Trajnimi mbi teknologji të reja:
   - Zbatimi i pajisjeve ose softuerëve të rinj për të siguruar që personeli është i aftë për përdorimin e tyre.
2. Testimi i procedurave të reja:
   - Verifikimi i protokolleve të reja të sigurisë kibernetike për të siguruar që ato funksionojnë sipas parashikimeve.
3. Ruajtja dhe përmirësimi i aftësive:
   - Sigurimi që aftësitë ekzistuese të stafit janë të freskëta dhe të përditësuara me praktikat më të mira.
4. Identifikimi i dobësive:
   - Eksplorimi i dobësive teknike dhe operacionale përmes simulimeve të fokusuara.

3.3.5.5 Stërvitje të Përbashkëta Ndërkombëtare

Stërvitjet e përbashkëta ndërkombëtare janë iniciativë strategjike për të rritur bashkëpunimin ndërmjet vendeve dhe organizatave në adresimin e kërcënimeve kibernetike globale. Duke sjellë së bashku ekspertë nga sektorë publikë dhe privatë, këto stërvitje synojnë të përmirësojnë koordinimin, shkëmbimin e informacionit dhe aftësitë për t'u përballur me incidente të ndërlikuara që kalojnë kufijtë kombëtarë.

Stërvitjet ndërkombëtare janë një element thelbësor për forcimin e sigurisë kibernetike. Ato ndihmojnë në ndërtimin e një infrastrukture më të fortë bashkëpunimi, rrisin ndërveprimin ndërmjet vendeve dhe sigurojnë që kërcënimet globale të përballohen në mënyrë efektive dhe të koordinuar. Me rritjen e kompleksitetit të kërcënimeve kibernetike, këto stërvitje bëhen gjithnjë e më të domosdoshme.

- **Përshkrimi:** Ushtrime bashkëpunuese me NATO-n, BE-në dhe partnerë rajonalë për të adresuar kërcënimet kibernetike ndërkufitare.
- **Frekuenca:** Planifikohen çdo vit për të forcuar rolin e Shqipërisë në përpjekjet rajonale dhe globale për sigurinë kibernetike.
- **Objektivat:** Përmirësimi i koordinimit, ndarja e inteligjencës mbi kërcënimet dhe aftësitë e përbashkëta për reagim.

3.4 Mirëmbajtja e planit

Plani Kombëtar për reagimin ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike është një dokument i cili duhet ta mbahet i përditësuar dhe i përshtatshëm për sfidat dhe kërcënimet e sigurisë kibernetike në zhvillim. Ai duhet të rishikohet dhe përditësohet rregullisht për të reflektuar legjislacionin dhe politikat ekzistuese dhe të reja, përvojat e fituara nga incidentet dhe testimet, si dhe për t'u përshtatur me kushtet dhe teknologjitë që evoluojnë vazhdimisht.
Plani Kombëtar për reagimin ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike do të rishikohet çdo 2 vjet në mënyrë që:

- Të identifikohen dobësitë dhe rreziqet e reja

- Të përshtatet me teknologjitë e reja
- Të ketë një qasje të përmirësuar ndërkombëtare, duke u përpjekur për harmonizim me protokollet ndërkombëtare dhe përforcimin e bashkëpunimit ndërkufitar në luftën kundër kërcënimeve kibernetike.
- Të ketë përmirësim të reagimit dhe aftësive pas incidenteve kibernetike ose simulimeve, pas bërjes së analizave të thelluara dhe mësimeve të nxjerra.
- Të reflektohet Vlerësimi Kombëtar i Rrezikut të Sigurisë Kibernetike.
- Të reflektohen ndryshimet në sistemin e paralajmërimit të hershëm
- Të përshtatet me ndryshimet ligjore dhe të politikave në fushën e sigurisë kibernetike

Gjatë rishikimit të zbatimit të Planit Kombëtar për reagimin ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike AKSK-ja do të marrë në konsideratë praktikat më efektive dhe mësimet e nxjerra nga ushtrimet, stërvitjet dhe incidentet kibernetike të mëparshme, si dhe do të vlerësojë proceset dhe teknologjitë e reja. Praktikat efektive përfshijnë planifikimin e vazhdimësisë së operacioneve kibernetike, të cilat garantojnë ruajtjen e masave të sigurisë, pavarësisht kërcënimeve dhe sulmeve. Proceset dhe teknologjitë e reja do të duhet të mundësojnë që Shqipëria të përshtatet në mënyrë efikase ndaj rreziqeve në zhvillim, të përdorë të dhëna për të kuptuar më mirë vendndodhjen, kontekstin dhe ndërvarësitë në infrastrukturat e saj kibernetike dhe të mundësojë një koordinim të shpejtë dhe efektiv në të gjitha nivelet e përgjigjes ndaj incidenteve kibernetike.

3.5 Burimet dhe Infrastrukturat

Zbatimi efektiv i Planit Kombëtar të reagimit ndaj incidenteve në shkallë të gjerë dhe krizave të sigurisë kibernetike mbështetet në burime dhe infrastruktura të fuqishme. Burimet teknike dhe financiare të mjaftueshme janë thelbësore për ndërtimin dhe mirëmbajtjen e një ekosistemi digjital të sigurt dhe të qëndrueshëm, ndërsa përmirësimi i infrastrukturës së sigurisë kibernetike siguron gatishmërinë e Shqipërisë për të adresuar dhe përballur kërcënimet kibernetike që evoluojnë.

Burimet Teknike dhe Financiare të Kërkuara

1. Burimet Teknike
   - Sistemet e Zbulimit të Kërcënimeve: Vendosja e mjeteve të avancuara për monitorim si sistemet Security Information and Event Management (SIEM), sistemet e zbulimit të ndërhyrjeve (IDS) dhe platformat e automatizuara të inteligjencës mbi kërcënimet.
   - Mjetet e Reagimit ndaj Incidenteve: Sigurimi i mjeteve për analizën e malware-ve, forenzikën digjitale dhe rikuperimin e të dhënave për të mundësuar reagime të shpejta dhe efikase ndaj incidenteve kibernetike.
   - Kanale të Sigurta Komunikimi: Krijimi i rrjeteve dhe platformave të koduara për komunikim të sigurt midis palëve të interesuara gjatë incidenteve dhe krizave kibernetike.
   - Sistemet e Kopjeve Rezervë dhe Rikuperimit: Zbatimi i zgjidhjeve të fuqishme për kopje rezervë të të dhënave për të siguruar integritetin dhe rikuperimin e shpejtë në rast sulmesh.
2. Burimet Financiare

- Alokimi i Buxhetit: Financim i dedikuar nga buxheti kombëtar për të mbështetur iniciativat e sigurisë kibernetike, përmirësimet e infrastrukturës dhe zhvillimin e ekspertëve të sigurisë kibernetike.
- Investimet Publiko-Private: Nxitja e kontributeve financiare nga sektori privat për të përmirësuar ekosistemin e përgjithshëm të sigurisë kibernetike.
- Financimi Ndërkombëtar: Shfrytëzimi i granteve dhe mbështetjes nga organizatat ndërkombëtare si dhe partnerët strategjik, duke përfshirë BE-në dhe NATO-n, për ndërtimin e kapaciteteve dhe blerjen e teknologjive.

3.6 Identifikimi i rrezikut, analiza e cenueshmërisë e ekspozimit dhe vlerësimi i riskut

Në kuadër të reagimit ndaj incidenteve kibernetike dhe krizave të mundshme, identifikimi i rrezikut, analiza e cenueshmërisë, vlerësimi i ekspozimit dhe vlerësimi i riskut janë elementë thelbësorë që sigurojnë një reagim efektiv dhe të shpejtë. Ky proces përfshin disa hapa të rëndësishëm, që lejojnë që infrastrukturat dhe autoritetet të jenë të përgatitura për t'u përballur me kërcënime të ndryshme në fushën e sigurisë kibernetike.

1. Identifikimi i Rrezikut

Identifikimi i rrezikut është një proces që përfshin vlerësimin e mundësisë së sulmeve kibernetike që mund të ndikojnë në infrastrukturat dhe shërbimet kritike. Ky proces përfshin:

- Përcaktimin e kërcënimeve të mundshme: Kjo përfshin sulme nga aktorë të jashtëm (hakerë, grupime kriminale) ose nga brenda (abuzime nga përdorues të autorizuar).
- Identifikimi i dobësive: Çdo sistem ka dobësi që mund të shfrytëzohen për të ndërhyrë. Kjo përfshin softuerët e paazhurnuar, mungesën e trajnimeve për stafin, dhe mangësitë e konfigurimeve të sigurisë.
- Vlerësimi i kërcënimeve kibernetike të mundshme: Identifikimi i llojeve të sulmeve të mundshme si malware, ransomware, DDoS, sulme phishing, etj.
- Përshkrimi i mundësive të sulmeve dhe aktivitetit të dyshimtë: Analiza e mundësive për sulme në infrastrukturat kritike dhe pasojat që mund të shkaktojnë ato.

2. Analiza e Cënueshmërisë

Analiza e cënueshmërisë përqendrohet në identifikimin e dobësive të sistemeve dhe infrastrukturave të informacionit që mund të ndikojnë në mbrojtjen dhe ruajtjen e integritetit të të dhënave. Ky proces përfshin:

- Përkufizimin e burimeve kritike: Identifikimi i sistemeve dhe të dhënave që janë thelbësore për funksionimin e një infrastrukture dhe që mund të bëhen objekt i sulmeve.
- Përshkrimin e dobësive të brendshme: Si për shembull, përdorimi i fjalëkalimeve të dobëta, akses i paautorizuar në sisteme kritike, apo mosnënshtrimi ndaj rregullave të sigurisë.
- Testimin dhe auditimin e sistemeve: Provimi i sigurisë së sistemeve për të zbuluar dobësitë që mund të shfrytëzohen nga sulmuesit.

3. Vlerësimi i Ekspozimit

Vlerësimi i ekspozimit përqendrohet në matjen e nivelit të ndjeshmërisë që ka një infrastrukturë ndaj kërcënimeve dhe sulmeve të mundshme. Ky proces përfshin:

- Analizën e ndjeshmërisë së informacionit dhe sistemeve: Sa më shumë informacion të jetë i aksesueshëm ose i ndjeshëm, aq më e madhe është mundësia e ekspozimit ndaj sulmeve kibernetike.
- Përshkrimi i mundësive të aksesit të jashtëm: Kjo përfshin lidhjet e mundshme të jashtme, si rrjetet e internetit dhe sistemet që janë të lidhura me sisteme të tjera ndërkombëtare ose institucionale.
- Vlerësimi i rrezikut të cenimit së të dhënave: Sa i ekspozuar është informacioni në situata kur ky informacion mund të manipulohet ose të vidhet.

4.Vlerësimi i Rrezikut

Vlerësimi i rrezikut është procesi i përmbledhjes dhe analizës së të dhënave për të përcaktuar ndikimin dhe mundësinë që një incident kibernetik të ndodhi, duke u përqendruar në pasojat e mundshme për sigurinë dhe stabilitetin e infrastrukturës dhe shërbimeve kritike. Ky proces përfshin:

- Vlerësimi i mundësisë dhe impaktit: Duke vlerësuar mundësinë që një sulm i caktuar të ndodhë dhe ndikimin që ai mund të ketë në sistemet dhe shërbimet kritike.
- Përzgjedhja e masave të menaxhimit të riskut: Identifikimi i masave që mund të ndërmerren për të zvogëluar mundësinë e ndodhjes së sulmeve dhe për të minimizuar impaktin e tyre.
- Prioritizimi i rrezikut: Vlerësimi i aspekteve të ndryshme të sigurisë dhe klasifikimi i kërcënimeve sipas mundësisë dhe rëndësisë, për të përcaktuar se cilat duhet të adresohen menjëherë dhe cilat mund të vonohen.

3.7 Masat në fazën e gatishmërisë

Falë informacionit, njohurive të specializuara, trajnimeve të përshtatura, paralajmërimit të hershëm dhe vlerësimit të riskut, gatishmëria për të përballuar emergjencat kibernetike duhet të sigurojë sisteme funksionale dhe reaguese. Këto sisteme duhet të jenë të pajisura me burime të mjaftueshme për të garantuar reagimin e duhur ndaj rreziqeve dhe incidenteve kibernetike.

Një qasje gjithëpërfshirëse dhe e koordinuar, që përfshin bashkëpunimin ndërinstitucional dhe përfshirjen e shoqërisë civile, është thelbësore për të siguruar një gjendje të lartë gatishmërie ndaj emergjencave kibernetike. Në këtë mënyrë, Shqipëria dhe infrastrukturat e saj mund të reagojnë në mënyrë të efektshme ndaj kërcënimeve dhe të sigurojnë qëndrueshmëri përballë rreziqve kibernetike.

3.8 Vazhdimësia e veprimtarisë dhe shërbimeve

Vazhdimësia e veprimtarisë dhe shërbimeve është një element thelbësor për mbrojtjen e infrastrukturave kritike, menaxhimin e incidenteve kibernetike dhe garantimin e funksionimit të pandërprerë të infrastrukturave. Ky koncept përfshin një set masash dhe procedurash që synojnë mbrojtjen e sistemeve, ruajtjen e integritetit të të dhënave dhe sigurinë e shërbimeve edhe në rast të sulmeve apo incidenteve kibernetike. Pjesë e këtij procesi është gjithashtu përgatitja për vazhdimin e operacioneve në kushte emergjente dhe rimëkëmbjen pas një krize të mundshme.

1. Planifikimi i Vazhdimësisë së Operacioneve

Planifikimi i vazhdimësisë së operacioneve është një proces që synon të sigurojë që infrastrukturat të mund të vazhdojnë të ofrojnë shërbime kritike edhe në situata të krizave. Ky plan duhet të përfshijë:

- Identifikimin e shërbimeve kritike: Këto janë shërbime që nuk mund të ndërpriten për shkak të rëndësisë së tyre për funksionimin e infrastrukturës ose për shërbimet ndaj qytetarëve dhe përdoruesve.
- Përgatitja e planeve për rimëkëmbjen: Plani i rimëkëmbjes nga emergjencat kibernetike përfshin procedura dhe teknika për rikthimin e sistemeve, shërbimeve dhe të dhënave pas një incidenti kibernetik.
- Sigurimi i burimeve dhe infrastrukturave alternative: Kjo përfshin përdorimin e burimeve alternative dhe sistemeve të mbështetjes për të siguruar funksionimin e pandërprerë të shërbimeve gjatë dhe pas krizave.

2. Menaxhimi i Rrezikut dhe Vazhdimësia e Shërbimeve

Një pjesë thelbësore e vazhdimësisë së veprimtarisë është menaxhimi i rrezikut, i cili përfshin:

- Identifikimin dhe vlerësimin e rreziqeve kibernetike: Infrastrukturat duhet të kuptojnë kërcënimet që mund të ndikojnë në vazhdimësinë e shërbimeve dhe t'i parandalojnë ato përpara se të ndodhin.
- Mbrojtja nga sulmet kibernetike: Përdorimi i masave të sigurisë si firewall, antivirus, sistemi i detektimit të depërtimit dhe encryption për të parandaluar ndërhyrjet në sisteme dhe shërbime.
- Kontrolli i pasojave të sulmeve: Në rast se një incident ndodh, duhet të merren masa për të kufizuar pasojat dhe për të siguruar vazhdimësinë e operacioneve përmes planeve të rimëkëmbjes.

3. Trajnimi dhe Testimi i Vazhdimësisë së Veprimtarisë

Përgatitja e stafit dhe strukturave për të reaguar ndaj krizave kibernetike është e rëndësishme për të garantuar një proces të suksesshëm të vazhdimësisë. Ky proces përfshin:

- Trajnimin e stafit: Stafi duhet të trajnohet për t'u përgjigjur shpejt dhe efektivisht ndaj incidenteve kibernetike dhe për të ditur si të menaxhojnë situatat emergjente.
- Ushtrimet dhe simulimet: Ushtrimet dhe testet janë thelbësore për të vlerësuar gatishmërinë e infrastrukturës për të ruajtur vazhdimësinë e shërbimeve dhe për të testuar planet dhe procedurat e rimëkëmbjes në kushte të ngjashme me ato reale.

4. Monitorimi dhe Përditësimi i Planit të Vazhdimësisë

Për të siguruar që një plan vazhdimësie të jetë gjithmonë i përshtatshëm dhe efektiv, është e nevojshme që ai të monitorohet dhe të përditësohet vazhdimisht, duke përfshirë:

- Monitorimi i sistemeve dhe shërbimeve: Kjo siguron që çdo dobësi ose rrezik i mundshëm të identifikohet dhe të merret masa për të minimizuar impaktin në vazhdimësinë e veprimtarisë.
- Përditësimi i planeve të sigurisë dhe rimëkëmbjes: Plani duhet të përditësohet në mënyrë të rregullt për të përfshirë teknologjitë e reja dhe kërcënimet që mund të ndodhin, duke garantuar që ai të mbetet efikas dhe i përshtatshëm për çdo situatë.

5. Bashkëpunimi dhe Koordinimi Ndërkombëtar

Vazhdimësia e shërbimeve dhe operacioneve kibernetike nuk është vetëm çështje e brendshme, por gjithashtu kërkon një koordinim të gjerë me partnerë ndërkombëtarë dhe agjenci të tjera. Ky koordinim përfshin:

- Ndihma ndërkombëtare dhe burime të përbashkëta: Nëse ndodhin incidente kibernetike të mëdha, kërkohet bashkëpunimi ndërkombëtar për të menaxhuar dhe për t'u rikuperuar shpejt.
- Standarde të përbashkëta dhe korniza ligjore: Adoptimi i standardeve të përbashkëta për sigurinë kibernetike dhe politika të harmonizuara për të siguruar vazhdimësinë e shërbimeve edhe përtej kufijve.

3.9 Rolet dhe përgjegjësitë e subjekteve përgjegjëse për sigurinë kibernetike në fazën e gatishmërisë

Për të menaxhuar incidentet kibernetike në nivel kombëtar duhet të përcaktohen rolet dhe përgjegjësitë e secilit aktor në fazën e Gatishmërisë, duke nisur nga nivelet më të larta drejtuese përfshirë:

1. Autoriteti Kombëtar i Sigurisë Kibernetike/ CSIRT Kombëtar;
2. Titullari i Institucionit;
3. CSIRT Sektorial;
4. CSIRT pranë operatorit ;
5. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

1. Autoriteti Kombëtar i Sigurisë Kibernetike/ CSIRT Kombëtar, Ekipi i Përgjigjes ndaj Emergjencave, është Autoritet me kompetenca rregullatore, koordinuese, dhe ushtron rolet dhe përgjegjësitë e mëposhtme:

a. Siguron zbatimin e politikave të sigurisë kibernetike bazuar në standardet e mirënjohura ndërkombëtare të sigurisë si dhe të ligjit nr.25/2024 “Për sigurinë kibernetike” dhe akteve nënligjore në zbatim të tij;
b. Mban në gatishmëri ekipin e përgjigjes ndaj incidenteve kibernetike/CSIRT-in Kombëtar si dhe udhëzon krijimin e ekipit të përgjigjes ndaj incidenteve kibernetike të operatorit/CSIRT pran operatorit;
c. Zhvillon trajnime në nivel kombëtar dhe ushtrime të rregullta simuluese për të siguruar një ekip të përgjigjes ndaj incidenteve kibernetike në nivel kombëtar të trajnuar dhe të gatshëm për t’ju përgjigjur incidentit, si dhe gjithashtu rishikon fazën e përgatitjes dhe dokumenton kërcënimet e reja ndërkohë që zbulohen;
ç. Siguron zbatimin e strategjive të përgjigjes që prioritizojnë rreziqet bazuar në rëndësinë e ndikimit të tyre;
d. Përditëson planin e detajuar të komunikimit për të informuar infrastrukturat, palët e interesuara dhe organet e zbatimit të ligjit rreth incidenteve kibernetike. Përcaktohen pikat e kontaktit për të gjithë anëtarët e ekipit të përgjigjes dhe sigurohet një rrjedhë komunikimi e kriptuar;
dh. Siguron si CSIRT kombëtar disponueshmërinë e mjeteve dhe zgjidhjeve të nevojshme për përgjigje ndaj incidenteve;

e. Siguron dhe udhëzon kontrollin e aksesit nëpërmjet zbatimit të masave dhe protokolleve të sigurisë me qëllim që të sigurohet vetëm aksesi i personave të autorizuar në burimet e ndjeshme.

2. Titullari i institucionit në cilësinë e titullarit të institucionit:

a. Drejtojnë institucionin e tyre për koordinimin e proceseve të nevojshme në fazën e gadishmërisë;
b. Informojnë CSIRT-in Kombëtar në mënyrë zyrtare mbi planin e komunikimit, disponueshmerine e mjeteve, zbatimin e masave kibernetike dhe protokolleve të sigurisë me qëllim që të sigurohet vetëm aksesi i personave të autorizuar në burimet e ndjeshme të shërbimeve në institucionin e tyre;

3. **CSIRT Sektorial**, në cilësine e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të sektorit përkatës:

a. Siguron rritje të kapaciteteve të stafit nëpërmjet trajnimeve dhe certifikimeve periodike sipas sektorëve që mbulojnë.

4. **CSIRT pranë operatorit** në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të operatorit përkatës:

a. Zbaton politika të sigurisë kibernetike bazuar në standardet e mirënjohura ndërkombëtare të sigurisë dhe aktet nënligjore në zbatim të ligjit nr.25/2024 "Për sigurinë kibernetike";
b. Mban në gatishmëri ekipin e përgjigjes ndaj incidenteve kibernetike/CSIRT-in pran operatorit;
c. Siguron trajnimin dhe pjesëmarrjen në ushtrime të rregullta simuluese për të siguruar një ekip të përgjigjes ndaj incidenteve kibernetike të trajnuar dhe të gatshëm për t'ju përgjigjur incidentit, si dhe gjithashtu rishikon fazat e përgatitjes dhe dokumenton kërcënimet e reja ndërkohë që zbulohen;
ç. Siguron zbatimin e strategjive të përgjigjes që prioritizojnë rreziqet bazuar në rëndësinë e ndikimit të tyre;
d. Përditëson planin e komunikimi për të informuar, palët e interesuara dhe organet e zbatimit të ligjit rreth incidenteve kibernetike. Përcaktohen pikat e kontaktit për të gjithë anëtarët e ekipit të përgjigjes dhe siguron një rrjedhë komunikimi e kriptuar;
dh. Siguron disponueshmërinë e mjeteve dhe zgjidhjeve të nevojshme për përgjigje ndaj incidenteve;
e. Siguron kontrollin e aksesit nëpërmjet zbatimit të masave dhe protokolleve të sigurisë me qëllim që të sigurohet vetëm aksesi i personave të autorizuar në burimet e ndjeshme.

5. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale në cilësinë e institucionit përgjegjës për hartimin e politikave për mbrojtjen e të dhënave personale të individëve, monitoron zbatimin e legjislacionit përkatës në rastin e incidenteve dhe krizës kibernetike:

a. Trajton, kontrollon, dhe monitoron zbatimin e legjislacionit ne fuqi mbi mbrojtjen e te dhënave personale.

Seksioni 4: Përgjigja

Faza e përgjigjes ndaj incidenteve kibernetike në shkallë të gjerë dhe krizave përfshin masa të koordinuara për të minimizuar ndikimin, rikuperuar sistemet e prekura dhe siguruar vazhdimësinë e operacioneve kritike. Ky proces kërkon përgatitje, ekzekutim të planifikuar dhe monitorim të vazhdueshëm.

Objektivat kryesore të fazës së Përgjigjes

- Minimizimi i dëmeve: Reduktimi i ndikimit të incidentit mbi sisteme, të dhëna dhe operacione.
- Sigurimi i transparencës: Ofrimi i informacionit të qartë dhe të besueshëm për palët e interesuara.
- Përgatitja për fazën e rikuperimit: Vendosja e bazave për rikthimin e qëndrueshmërisë dhe përmirësimin e sistemeve për të parandaluar incidente të ardhshme.

Kjo fazë është thelbësore për të siguruar një reagim të shpejtë dhe efektiv ndaj krizave, duke minimizuar ndërprerjet dhe duke mbrojtur interesat kombëtare dhe ndërkombëtare.

4.1 Mbledhja e informacionit dhe menaxhimi i të dhënave

Mbledhja e informacionit dhe menaxhimi i të dhënave në rastet e incidenteve të sigurisë kibernetike me shkallë të gjerë është një proces i rëndësishëm për të siguruar një reagim të shpejtë, të koordinuar dhe efikas. Ky proces përfshin mbledhjen, analizën dhe ruajtjen e të dhënave dhe informacionit që mund të ndihmojnë në identifikimin, zbutjen dhe rikuperimin e pasojave të incidenteve. Mbledhja e informacionit dhe menaxhimi i të dhënave janë shtyllat kryesore të një përgjigjeje efektive ndaj krizave kibernetike. Me integrimin e IA dhe teknologjive të tjera të avancuara, infrastrukturat mund të përmirësojnë shpejtësinë, saktësinë dhe efikasitetin e tyre për të përballuar kërcënimet komplekse dhe të vazhdueshme. Elementët kyç për mbledhjen e informacionit dhe menaxhimin e të dhënave janë si vijon:

1. Mbledhja e të dhënave në kohë reale

- Përdorimi i sistemeve të monitorimit të sigurisë ndihmon për të mbledhur informacionin në kohë reale. Këto sisteme mund të identifikojnë aktivitete të dyshimta në rrjet dhe mund të regjistrojnë të dhënat e lidhura me incidentet e mundshme, si adresat IP të dyshimta, kërkesat anormale, dhe lëvizjet e paautorizuara të të dhënave.
- Aktivitetet në sisteme dhe servera duhet të regjistrohen për të krijuar një gjurmë të plotë të asaj që ka ndodhur. Kjo mund të përfshijë log-et e sistemeve, log-et e rrjetit dhe regjistrat e ngjarjeve të sigurisë.

2. Klasifikimi dhe filtrimi i të dhënave

- Pasi informacioni është mbledhur, është e rëndësishme që të klasifikohet për të dalluar informacionin e rëndësishëm nga ai që nuk është i nevojshëm. Ky klasifikim mund të përfshijë ndarjen e të dhënave në kategori si: të dhëna të ndjeshme, informacion për kërcënime, aktivitete të dyshimta, etj.
- Të dhënat duhet të filtrohen, kjo pasi jo të gjitha të dhënat janë të nevojshme për analizë. Filtrimi i të dhënave për të identifikuar informacionin më të rëndësishëm, ndihmon në hetimin e incidentit dhe mund të ndihmojë në gjetjen e burimit të sulmit.

3. Ruajtja dhe sigurimi i të dhënave

- Të dhënat e mbledhura nga incidentet kibernetike duhet të ruhen në mënyrë të sigurt, në mënyrë që të mund të analizohen në të ardhmen dhe të përdoren si prova nëse është e nevojshme. Ruajtja mund të përfshijë përdorimin e serverëve të veçantë të siguruar, duke përdorur enkriptimin dhe kontrollet e aksesit për të mbajtur të dhënat të papërshkueshme.
- Është e rëndësishme që të dhënat të ruhet me integritet të plotë. Kjo do të thotë që ato nuk duhet të mund të manipulohen ose modifikohen nga palë të treta pa autorizim. Përdorimi i metodave si hash dhe kontrolle të integritetit mund të ndihmojë në sigurimin e këtyre të dhënave.

4. Analiza e të dhënave dhe identifikimi i kërcënimeve

- Pasi të dhënat janë mbledhur dhe ruajtur, ato duhet të analizohen për të kuptuar natyrën dhe shkallën e incidentit. Përdorimi i mjeteve të analizës për të identifikuar karakteristikat e dyshimta, si dhe për të kuptuar se si janë kompromet uar sistemet dhe rrjetet e informacionit.
- Përdorimi i *threat intelligence* është një proces që përfshin mbledhjen e informacionit të jashtëm për kërcënimet aktuale dhe përdorimin e tij për të përmirësuar reagimin ndaj incidentit.

5. Koordinimi me palë të treta dhe partnerë

- Në raste të incidenteve me shkallë të gjerë, siç janë sulmet kibernetike të financuara ose të mbështetura nga shteti, mund të jetë e nevojshme që të koordinoheni me strukturat e sigurisë kibernetike, partnerët dhe institucionet ndërkombëtare. Këto mund të ndihmojnë në mbledhjen e informacionit dhe koordinimin e përgjigjes.
- Shumë incidente të sigurisë kibernetike përfshijnë partnerë, dhe mbledhja e informacionit dhe menaxhimi i të dhënave duhet të përfshijë gjithashtu këto palë për të zbuluar burimin e sulmit dhe për të parandaluar përhapjen e tij.

4.1.1 Informimi dhe ndërgjegjësimi mbi rreziqet

Në një krizë kibernetike, informimi dhe ndërgjegjësimi i palëve të përfshira është një komponent i rëndësishëm për të siguruar një reagim të shpejtë, të koordinuar dhe të efektshëm. Kjo fazë kërkon komunikim strategjik, përgatitje për të edukuar përdoruesit dhe për të parandaluar përhapjen e mëtejshme të dëmeve. Informimi dhe ndërgjegjësimi janë kritike për të minimizuar ndikimin e incidenteve kibernetike në shkallë të gjerë dhe krizës kibernetike. Përmes strategjive të mira komunikimi dhe përdorimit të teknologjive të avancuara, infrastrukturat mund të reagojnë më mirë dhe të mbrojnë interesat e tyre gjatë një krize.

Roli i Informimit dhe Ndërgjegjësimit

Informimi dhe ndërgjegjësimi ndihmojnë në:

- Minimizimin e panikut: Shpjegimi i situatës në mënyrë të qartë për të parandaluar keqkuptimet dhe përhapjen e frikës.
- Përmirësimin e vendimmarrjes: Furnizimi i informacionit të saktë dhe të detajuar për të ndihmuar drejtuesit dhe ekipet të marrin masa të duhura.
- Parandalimin e përhapjes së kërcënimeve: Edukimi i përdoruesve për të mos kryer veprime që mund të përkeqësojnë situatën (si hapja e e-maileve të dyshimta).

4.1.2 Njohuritë mbi situatën

Njohuritë mbi situatën janë thelbësore për menaxhimin dhe reagimin ndaj incidenteve kibernetike në shkallë të gjerë dhe krizës kibernetike të cilat përfshijnë aftësinë për të:

- **Identifikuar** gjendjen aktuale të rrjetit, sistemeve dhe burimeve.
- **Kuptuar** ndikimin e një incidenti në organizatë dhe në interesat e saj.
- **Parashikuar** përshkallëzimin e mundshëm të kërcënimeve dhe efektet e masave të reagimit.

Njohuritë mbi situatën janë themeli i një reagimi të suksesshëm ndaj incidenteve kibernetike me shkallë të gjerë dhe krizës kibernetike. Infrastrukturat që investojnë në teknologji moderne, trajnime dhe forcojnë bashkëpunimin mund të ndërtojnë një kapacitet më të mirë për të kuptuar, menaxhuar dhe parandaluar kërcënimet kibernetike.

Rëndësia e njohurive mbi situatën për menaxhimin dhe reagimin ndaj incidenteve kibernetike në shkallë të gjerë dhe krizës kibernetike:

- Siguron informacion për të përmirësuar vendimmarrjen.
- Mundëson reagim të shpejtë dhe të koordinuar ndaj incidenteve.
- Ndihmon në përcaktimin e prioriteteve dhe alokimin e burimeve.

Fazat e njohurive mbi situatën për menaxhimin dhe reagimin ndaj incidenteve kibernetike në shkallë të gjerë dhe krizës kibernetike janë si vijojnë:

1. Mbledhja e Informacionit
   - Mbledhja e informacionit nga burime të shumta, duke përfshirë logjet e sistemeve, analizën e trafikut të rrjetit dhe raportimet nga palët e interesuara.
   - Përdorimi i platformave të inteligjencës së kërcënimeve për të marrë informacion mbi tendencat globale të sulmeve.
2. Kuptimi i Informacionit
   - Analiza e të dhënave të mbledhura për të ndërtuar një kuptim të qartë të rrezikut dhe ndikimit të incidentit.
   - Klasifikimi i informacionit për të përcaktuar prioritetet dhe për të optimizuar burimet.
3. Parashikimi
   - Parashikimi i zhvillimit të mundshëm të situatës duke përdorur analiza historike dhe modele të mësimit të makinerive.
   - Planifikimi i masave për të parandaluar përshkallëzimin e krizës dhe për të rikthyer operacionet në normalitet.

4.2 Aktivizimi i përgjigjes në Shqipëri

Me rritjen e sulmeve kibernetike dhe ndikimin e tyre në infrastrukturat kritike, Shqipëria ka përqafuar një qasje të strukturuar për të trajtuar incidentet e sigurisë kibernetike dhe krizave në këtë fushë. Ky proces përfshin mekanizma ligjorë, teknologjikë dhe organizativë që synojnë të sigurojnë një përgjigje të shpejtë dhe efektive ndaj kërcënimeve kibernetike.

Aktivizimi i përgjigjes në Shqipëri në rastet e incidenteve kibernetike me shkallë të gjerë përfshin një seri hapash të koordinuar dhe masash të menjëhershme, të cilat janë të domosdoshme për të menaxhuar dhe zvogëluar ndikimin e mundshëm të këtyre incidenteve.

Ky proces kërkon angazhim të institucioneve shtetërore, sektorëve të përfshirë, si dhe një bashkëpunim ndërmjet aktorëve të ndryshëm të sigurisë kibernetike. Disa nga elementët kyç që përfshihen në aktivizimin e përgjigjes në rastet e incidenteve kibernetike me shkallë të gjerë dhe krizës kibernetike në Shqipëri:

1. **Detektimi i incidentit dhe aktivizimi i grupit të reagimit**
   - Kur një incident i mundshëm kibernetik i shkallës së gjerë identifikohet, ekipi i përgjigjes ndaj emergjencave, CERT, aktivizohet menjëherë për të vlerësuar incidentin dhe për të hartuar planin e masave që duhet të merren për parandalimin e përhapjes dhe minimizimin e dëmit.
2. **Koordinimi** me aktorët kombëtarë dhe ndërkombëtarë
   - Koordinimi me strukturat kombëtare të sigurisë në mënyrë që të parandalohet shpërndarja e mëtejshme e kërcënimit.
   - Bashkëpunimi me partnerë ndërkombëtarë të sigurisë kibernetike, për shkëmbimin e informacionit dhe kërkimin e ndihmës.
3. **Menaxhimi i komunikimit**
   - Përcaktimi qartë i mesazheve për publikun dhe palët e interesuara, për të shmangur panikun dhe për të siguruar transparencë mbi masat që po merren.
4. **Minimizimi i dëmit dhe rikuperimi i sistemeve**
   - Pasi është realizuar një vlerësim i plotë dhe kërcënimi është neutralizuar, nis procesi i rikuperimit të të dhënave të humbura ose të dëmtuara. Ky proces duhet të bëhet me kujdes dhe duke u siguruar që të gjitha sistemet janë të pastra nga çdo kërcënim i mundshëm.
5. **Vlerësimi dhe mësimet e nxjerra**
   - Pas përfundimit të reagimit ndaj incidentit, është thelbësore të kryhet një analizë e plotë e tij, për të kuptuar se si ndodhi dhe si mund të parandalohet në të ardhmen. Kjo përfshin një hetim të thellë të shkaqeve të incidentit dhe përmirësimin e politikave dhe procedurave për përgjigje ndaj incidenteve.
   - Pas incidentit, është e rëndësishme që të identifikohen boshllëqet në masat e sigurisë dhe të ndërmerren hapa për të rritur kapacitetet e sigurisë kibernetike në të ardhmen. Kjo mund të përfshijë trajnime të vazhdueshme për stafin, forcimin e infrastrukturës dhe përmirësimin e politikave të sigurisë.

4.3 Burimet dhe kapacitetet kombëtare për përgjigjen në situatat e incidenteve në shkallë të gjerë dhe Krizës Kibernetike në Shqipëri

Përballimi i krizave kibernetike kërkon koordinim të mirëfilltë dhe shfrytëzimin e burimeve dhe kapaciteteve kombëtare në të gjithë sektorët. Ministritë, institucionet shtetërore, strukturat operacionale dhe aktorët joqeveritarë kanë kapacitete specifike, të cilat duhet të integrohen në një qasje gjithëpërfshirëse për të siguruar një përgjigje efektive ndaj krizave kibernetike.

4.3.1 Subjektet përgjegjëse

1. Këshilli i Ministrave;
2. Kryeministri;
3. Komiteti Ndërministror i Sigurisë Kibernetike;
4. Ministrat;
5. Autoriteti Kombëtar i Sigurisë Kibernetike/ CSIRT Kombëtar;

6. CERT/ Ekipi i Përgjigjes ndaj Emergjencave, Krizës Kibernetike;
7. Titullari i Institucionit;
8. CSIRT Sektorial;
9. CSIRT pranë operatorit ;
10. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.
11. Policia e Shtetit.

4.3. 2 Informimi i publikut

Informimi i publikut në fazën e parë të një krize kibernetike është një element kyç për të minimizuar dëmet dhe për të ruajtur besimin e publikut. Në këtë fazë, theksi vihet në komunikimin e shpejtë, të qartë dhe transparent. Për të siguruar një informim efektiv duhet të krijohet nje plan i komunikimit për kriza kibernetike me protokolle të mirëpërcaktuar për informimin e publikut si dhe ngritjen e ekipit të komunikimit si dhe është e rëndësishme të:

- Identifikohet audienca ku përshihet publiku i interesuar, qytetarët e prekur, bizneset, punonjësit, mediat dhe palët e tjera të interesuara;
- Përdoren kanale të përshtatshme komunikimi, si media sociale, faqet zyrtare të internetit, aplikacione të dedikuara dhe televizioni;
- Sigurohet transparencë, qartësi, si dhe premtimi për informacione të mëtejshme;
- Ofrohen udhëzimeve konkrete, si për shembull: ndryshimi i fjalëkalimeve, mbyllja e llogarive të komprometuara, ose raportimi i incidenteve;
- Shmanget paniku si dhe fokusimi në sigurinë e publikut dhe zgjidhjen e situatës;
- Monitorohet reagimi i publiku, për të monitoruar perceptimin publik dhe përhapjen e dezinformatave.

4.3. 3 Raportimi

Raportimi është një element thelbësor i komunikimit dhe koordinimit gjatë reagimit ndaj incidenteve në shkallë të gjere dhe krizave kibernetike. Ai realizohet në përputhje me strukturat e përgjegjëse të sigurisë kibernetike sipas legjislacionit në fuqi për sigurinë kibernetike. Për të siguruar një proces të standardizuar, përdoren formularë dhe procedura të përcaktuara që ndihmojnë në mbledhjen dhe ndarjen e informacionit në mënyrë efikase.
Mënyra e raportimit do të bëhet sipas afateve dhe formateve standarde të miratuara nga Autoriteti Kombëtar për Sigurinë Kibernetike sipas rregullores për kategorizimin e incidenteve të sigurisë kibernetike. Detyrimin për raportim e kanë të gjithë operatorët e infrastrukturave të informacionit në momentin e identifikimit të një incidenti të sigurisë kibernetike.

4.3. 4 Shqyrtimet pas veprimeve

Shqyrtimet pas veprimeve janë një hap i rëndësishëm pas ndodhjes së një incidenti me shkallë të gjerë dhe krize kibernetike. Ky proces ndihmon për të vlerësuar se si është menaxhuar incidenti dhe identifikon mundësitë për përmirësimin e përgjigjes dhe parandalimin e ngjarjeve të ngjashme në të ardhmen. Shqyrtimi pas veprimeve përfshin analizën e detajuar të të gjitha fazave të incidentit dhe të përgjigjes ndaj tij, duke u fokusuar në mësimet e nxjerra dhe përmirësimet e mundshme. Disa element kyçe të shqyrtimit pas veprimeve janë si vijon:

1. Analiza e menaxhimit të incidentit

- Vlerësohet sa shpejt dhe në mënyrë efikase janë aktivizuar strukturat përgjegjëse për sigurinë kibernetike. A janë aktivizuar në kohën e duhur?
- Shqyrtohet se si është menaxhuar komunikimi nga strukturat përkatëse dhe përdoruesit. A ka pasur ndonjë problem në përcjelljen e informacionit në kohë reale? A janë përdorur mjetet e duhura për komunikim?

2. Vlerësimi i efektshmërisë së masave të marra

- Analizohet sa efektive kanë qenë masat e marra për të ndaluar përhapjen e incidentit. A janë zbatuar protokollet për mbrojtjen e të dhënave dhe sistemeve?
- Vlerësohet efikasiteti i masave të ndërmarra për të rikthyer shërbimet dhe sistemet në normalitet. Sa kohë ka zgjatur rikuperimi?

3. Identifikimi i dobësive

- Shqyrtohet se cilat dobësi të sistemeve, procedurave, ose politikave kanë lejuar që incidenti të ndodhë ose të përhapet. A ka pasur mosrespektim të praktikave më të mira të sigurisë? A janë përdorur teknologji të përparuara për mbrojtje?
- A janë protokollet dhe planet e sigurisë të përditësuara dhe të përshtatura me kërcënimet aktuale? A janë ato të mjaftueshme për t'u përballur me një incident të ngjashëm në të ardhmen?

4. Mësime të nxjerra dhe përshtatje e planit të sigurisë

- Identifikohen mësimet kryesore të nxjerra nga trajtimi i incidentit. Çfarë mund të bëhet më mirë për të parandaluar ngjarje të ngjashme në të ardhmen? Cilat janë dobësitë që kërkojnë përmirësim?
- Bazuar në mësimet e nxjerra, institucionet, infrastrukturat e informacionit duhet të përmirësojë planet dhe protokollet e sigurisë. Kjo mund të përfshijë përditësimin e politikave të reagimit ndaj incidenteve, trajnimin e stafit, dhe forcimin e masave mbrojtëse.

5. Vlerësimi i rekomandimeve dhe masave parandaluese

- Pas shqyrtimit të incidentit, identifikohen rekomandime për përmirësimin e infrastrukturës së informacionit dhe sigurisë.
- Rritja e trajnimit dhe edukimit të punonjësve, për t'i përgatitur ata për të njohur dhe reaguar ndaj kërcënimeve të sigurisë kibernetike.

6. Dokumentimi dhe raportimi pas incidentit

- Një raport i detajuar pas incidentit duhet të përfshijë një analizë të plotë të ngjarjes, përfshirë shkakun, pasojat, dhe masat që janë ndërmarrë për trajtimin e tij. Ky raport duhet të jetë i detajuar dhe të ofrojë rekomandime për veprimet e ardhshme.
- Dokumentimi i pas incidentit ndihmon për të krijuar një bazë për hetimet e ardhshme dhe për të zhvilluar strategji më të mira për të menaxhuar ngjarje të ngjashme.

4.3.5 Rishikimi

Rishikimi pas një incidenti me shkallë të gjerë dhe krize kibernetike është një proces i rëndësishëm që synon vlerësimin e menaxhimit të incidentit dhe identifikimin e mundësive për përmirësimin e përgjigjes dhe mbrojtjes në të ardhmen. Ky rishikim është thelbësor për të kuptuar si janë zbatuar politikat, procedurat dhe masat e sigurisë, si dhe për të mësuar nga ngjarja për të parandaluar incidente të tjera. Ky rishikim duhet të përfshijë të gjithë aktorët e

përfshirë në menaxhimin e krizave kibernetike dhe të analizojë se si janë realizuar masat e planifikuara, si dhe të sugjerojë veprime për përmirësimin e gatishmërisë dhe efikasitetit të përgjigjes për të ardhmen. Ky proces duhet të ndihmojë në identifikimin e dobësive dhe forcave të strukturave që kanë reaguar ndaj krizës kibernetike.

Rishikimi dhe Përmirësimi konsiston në:

1. Përmirësimin e masave të gatishmërisë: Bazuar në përfundimet e rishikimit, mund të rekomandohen përmirësime në masat parandaluese dhe lehtësuese, si dhe forcimi i kapaciteteve të përgjigjes ndaj incidenteve kibernetike.
2. Rishikimin e procedurave të komunikimit: Përshtatja e protokolleve të komunikimit për të siguruar që informatat e ndjeshme të mbeten të sigurta dhe të shpërndahen në mënyrë të shpejtë dhe efikase.
3. Përforcimin e bashkëpunimit ndërinstitucional dhe ndërkombëtar: Rritja e nivelit të bashkëpunimit me agjencitë ndërkombëtare dhe sektorët privatë për përmirësimin e përgjigjes ndaj krizave kibernetike.
4. Trajnimin dhe simulimeve: Organizimi i trajnimeve dhe simulimeve të rregullta për të testuar procedurat e reagimit dhe për të përmirësuar përgatitjen e ekipeve për krizën kibernetike.

4.3.6 Rolet dhe përgjegjësitë e subjekteve përgjegjëse për sigurinë kibernetike në fazën e përgjigjes.

1. **Këshilli i Ministrave** në cilësinë e organit kolegjial me propozim të Kryeministrit të vendit merr vendim për:

a. Shpalljen e krizës kibernetike për një periudhë 7 ditore.
b. Zgjatjen e periudhës së krizës por jo më shumë se 30 ditë.

2. Kryeministri në cilësinë e drejtuesit kryesor, drejton dhe koordinon të gjitha veprimet institucionale dhe ndër-institucionale shtetërore për koordinimin e të gjitha ministrave dhe institucioneve sikurse parashikohet në nenin 11, shkronja “a”/i-ix të ligjit nr.25/2024 “Për sigurinë kibernetike” në rastin e krizës kibernetikës dhe i paraqet Këshillit të Ministrave propozimin për:

a. Shpalljen e krizës kibernetike për një periudhë 7 ditore.
b. Zgjatjen e periudhës së krizës por jo më shumë se 30 ditë.

3. Komiteti Ndërministror i Sigurisë Kibernetike, në cilësinë e një Organi konsultativ për çështjet e sigurisë kibernetike, i cili drejtohet t nga Zëvendës-kryeministri i vendit, në rast krize koordinon punën midis ministrive, institucioneve, pjesë e Komitetit Ndërministror si dhe siguron konsultimin dhe koordinimin në raste të incidenteve/krizës kibernetike.

4. Ministri në cilësinë e organit individual luan rol drejtues dhe koordinues për institucionin/institucionet e varësisë në raste të incidenteve/krizës kibernetike si dhe i raporton kryeministrit. Gjithashtu merr vendimmarrje të rëndësishme.

5. **Autoriteti Kombëtar i Sigurisë Kibernetike**/ CSIRT Kombëtar/ CERT (Ekipi i Përgjigjes ndaj Emergjencave, Krizës Kibernetike) është Autoritet me kompetenca rregullatore, koordinuese, Ekipi i Përgjigjes ndaj incidenteve, Krizës Kibernetike dhe ushtron rolet dhe përgjegjësitë e mëposhtme:

a. I propozon Kryeministrit në koordinim me Institucionet e sigurisë dhe mbrojtjes sikurse parashikohet në nenin 11, shkronja "a" te ligjit nr.25/2024 "Për sigurinë kibernetike", shpalljen e gjendjes së krizës së sigurisë kibernetike dhe masat emergjente për zgjidhjen e situatës;
b. Krijon strukturën ad-hoc CERT;
c. Koordinon menaxhimin e krizës;
ç. Nxjerr vendime me karakter të përgjithshëm ose merr masa mbrojtëse të natyrës së përgjithshme;
d. Njofton zyrtarisht policinë e shtetit.

6. CERT, Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike
Është një strukturë ad-hoc që vepron si linjë e parë e mbrojtjes për trajtimin e emergjencave dhe krizës së sigurisë kibernetike.
Detyrat kryesore:

a. Koordinimi dhe ndërhyrja e shpejtë për trajtimin e incidenteve në shkallë të gjerë dhe krizave kibernetike.
b. Hartimin e planit të masave të emergjencës.
c. Menaxhimi dhe zgjidhja e emergjencës.

7. Titullari i institucionit në cilësinë e titullarit të institucionit

a. Drejtojnë institucionin e tyre për koordinimin e proceseve të nevojshme për menaxhimin e situatës së brendshme;
b. Informojnë në mënyrë zyrtare situatën kibernetike të shërbimeve të prekura në institucionin e tyre të shoqëruara me efektet financiare, shoqërore, shëndetësore, dhe ambjentale si pasoj e sulmit kibernetik:
    i. CSIRT-in Kombëtar;
    ii. CSIRT-in Sektorial përkatës;
    iii. Policinë e Shtetit;
    iv. Komisionerin për mbrojtjen e të dhënave personale
    v. Ministrin e linjës (opsionale)
    vi. Institucionet e shërbimeve sekrete (opsionale)
    vii. Institucionet ligj Zbatuese (opsionale)
c. Koordinohen me CSIRT Kombëtar, CSIRT Sektorial dhe palët e interesuara direkt në biznes;
ç. Koordinohen me median për ofrimin e informacionit lidhur me situatën

8. CSIRT Sektorial, në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të sektorit përkatës:

a. Raporton incidentin e ndodhur në infrastrukturat e sektorit pranë CSIRT-t kombëtar , Policisë se Shtetit, Komisionerin për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale;
b. Koordinon me CSIRT-et pranë operatorëve për t'iu përgjigjur situatës.

9. **CSIRT pranë operatorit** në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të operatorit përkatës:
   a. Raporton incidentin e ndodhur në infrastrukturat e operatorit përkatës pranë CSIRT-t kombëtar dhe CSIRT Sektorial, Policinë e Shtetit, Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale
   b. Koordinon me CSIRT-tet pranë operatorëve për tju përgjigjur situatës.

10. **Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale** në cilësinë e institucionit përgjegjës për hartimin e politikave për mbrojtjen e të dhënave personale të individëve, monitoron zbatimin e legjislacionit përkatës në rastin e incidenteve dhe krizës kibernetike:
   a. Trajton, kontrollon, dhe monitoron zbatimin e legjislacionit ne fuqi mbi mbrojtjen e të dhënave personale.
11. **Policia e Shtetit** në cilësinë e institucionit përgjegjës për hetimin e krimit kibernetik zbatimit të legjislacionit të fushës penale kryen këto veprime:
   a. Ndjek veprimet e nevojshme operacionale ne kuadër te zbatimit te legjislacionit te fushës penale.
   b. Bashkëpunon me CSIRT-in Kombëtar dhe atë pranë operatorit për analizën dhe hetimin e incidentit kibernetik
   c. Realizon veprimet procedurale ne kuadër te zbatimit te legjislacionit të fushës penale.

Seksioni 5 Rimëkëmbja

Rimëkëmbja e Shërbimeve pas Incidenteve në Shkallë të Gjerë dhe Krizës Kibernetike është një proces thelbësor që ndihmon infrastrukturat të kthehen në normalitet pas një ngjarjeje kibernetike të rëndë. Ky proces është i ndarë në disa faza dhe kërkon një qasje të koordinuar dhe të mirë-strukturuar për të siguruar që shërbimet të rikthehen në mënyrë të sigurt dhe të shpejtë, dhe për të minimizuar ndjeshëm ndikimet afatgjata të incidentit.

5.1. Rimëkëmbja e shërbimeve pas incidenteve në shkallë të gjerë dhe krizës Kibernetike

Rimëkëmbja në rastet e incidenteve me shkallë të gjerë është një proces i rëndësishëm që ka për qëllim rikthimin e operacioneve dhe funksioneve të infrastrukturës në një gjendje të qëndrueshme pas një incidenti në shkallë të gjerë. Ky proces është i lidhur ngushtë me sigurimin e vazhdimësisë së aktivitetit dhe rikthimin e sigurisë për të minimizuar ndikimet afatgjata të incidentit. Rimëkëmbja nuk është një hap i vetëm, por një seri veprimesh të koordinuara që ndihmojnë në rivendosjen e sistemeve, shërbimeve dhe infrastrukturës, si dhe në përmirësimin e gatishmërisë për incidentet e ardhshme.

1. **Rikuperimi i sistemeve dhe infrastrukturës**

- Pas identifikimit të incidenteve dhe marrjes së masave për ndalimin e përhapjes së ndikimeve, hapi i parë është rikthimi i sistemeve kritike. Kjo mund të përfshijë:
  - Rivendosjen e të dhënave nga kopja rezervë (backup).
  - Rikthimin e shërbimeve të prekura.
  - Përmirësimin e integritetit të sistemeve të sigurisë.
  - Pas rikthimit të sistemeve dhe shërbimeve, është e rëndësishme të kryhen kontrolle dhe testime për të siguruar që ato po funksionojnë në normalitet dhe të mos përsëriten në të ardhmen.

2. **Testimi dhe Verifikimi i Sigurisë**

Pas rikthimit të sistemeve, është e rëndësishme të realizohen testime të sigurisë, duke përfshirë kontrollin e të gjitha masave mbrojtëse dhe përditësimin e tyre nëse është e nevojshme. Ky testim mund të përfshijë:

- Testimin e firewall-eve dhe sistemeve të monitorimit.
- Testime të sigurisë për të zbuluar çdo dobësi të mundshme.
- Kontrollin e mbrojtjes ndaj kërcënimeve të reja, si viruse, sulme DDoS, etj.

3. Komunikimi dhe menaxhimi i informacionit

- Pas incidentit, është e rëndësishme të vazhdojë një komunikim për të informuar të gjithë për statusin e rimëkëmbjes dhe çdo zhvillim të ri. Ky komunikim duhet të jetë i shpejtë dhe i koordinuar, sidomos për ata që janë pjesë e ekipit të menaxhimit të krizës dhe përgjigjes ndaj incidentit.
- Komunikimi duhet të jetë transparent dhe të përfshijë informacion të qartë për masat që janë ndërmarrë, si dhe afatet për rikthimin e shërbimeve.

4. Analiza e pasojave dhe vlerësimi i dëmit

- Pas përfundimit të rimëkëmbjes, është e rëndësishme të bëhet një vlerësim i plotë i pasojave të incidentit. Ky proces ndihmon për të kuptuar se sa i rëndë ka qenë dëmi, cila ka qenë shkalla dhe si do të trajtohen dëmet afatshkurtra dhe afatgjata.
- Vlerësimi i pasojave është i rëndësishëm për të planifikuar dhe për të përmirësuar gatishmërinë për incidentet në të ardhmen.

5. Përmirësimi i gatishmërisë për incidentet e ardhshme

- Pas përfundimit të rimëkëmbjes, duhet të rishikohet dhe përditësohet plani i vazhdimësisë së aktivitetit të infrastrukturës. Ky plan duhet të jetë i përditësuar për të pasqyruar mësimet e nxjerra nga incidenti dhe për të adresuar çdo dobësi të identifikuar.
- Të adresohen dhe të përmirësohen dobësitë për të parandaluar incidente të ngjashme në të ardhmen.
- Ushtrimet dhe simulimet janë të rëndësishme për përgatitjen e infrastrukturave për incidente në të ardhmen. Pas një incidenti me shkallë të gjerë, është e rëndësishme që të bëhen testime të reja të gatishmërisë për t'u siguruar dhe përgatitur për të menaxhuar ngjarje të tjera.

5.2 Rolet dhe përgjegjësitë e subjekteve përgjegjëse për sigurinë kibernetike në fazën e rimëkëmbjes

Për të menaxhuar incidentet kibernetike në nivel kombëtar duhet të përcaktohen rolet dhe përgjegjësitë e secilit aktor në fazën e rimëkëmbjes, duke nisur nga nivelet më të larta drejtuese përfshirë:

1. Autoriteti Kombëtar i Sigurisë Kibernetike/ CSIRT Kombëtar;
2. Titullari i Institucionit;
3. CSIRT Sektorial;
4. CSIRT pranë operatorit;
5. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale.

1. **Autoriteti Kombëtar i Sigurisë Kibernetike**/CSIRT Kombëtar, Ekipi i Përgjigjes ndaj Emergjencave, është Autoritet me kompetenca rregullatore, koordinuese, dhe ushtron rolet dhe përgjegjësitë e mëposhtme:

a. Suporton operatorin e infrastrukturës për të rikthyer shërbimet dhe të dhënat në gjendjen e tyre normale dhe orienton përdorimin e mjeteve dhe teknikave për të përjashtuar kërcënimet dhe për të riparuar dëmet e shkaktuara si dhe izolimin e pajisjeve fundore dhe sistemeve të prekura për të parandaluar dëmtime të mëtejshme.
b. Suporton operatorin e infrastrukturës për pastrimin e komponentëve të incidentit në sistemet e prekura, si fshirja e skedarëve keqdashës, çaktivizim i llogarisë së përdoruesit, etj, sipas kategorisë së incidentit.
c. Suporton operatorin për të eliminuar kërcënimet kibernetike duke çaktivizuar sistemet e infektuara, duke skanuar për malware dhe duke adresuar vulnerabilitetet;
ç. Suporton operatorin për rikthimin në gjendjen e tyre para kompromentimit duke përdorur kopje rezervë të pastra. Gjithashtu i kërkon operatorit të bëjë monitorim për aktivitete të dyshimta dhe zbatohen arnimet e sigurisë për të adresuar dobësitë që shkaktuan ndërhyrjen.

2. Titullari i institucionit në cilësinë e titullarit të institucionit:

a. Drejtojnë institucionin e tyre për koordinimin e proceseve të nevojshme në fazën e rimëkëmbjes;
b. Siguron kryerjen e aktiviteteve në bashkëpunim me CSIRT-in Kombëtar për të rikthyer shërbimet dhe të dhënat në gjendjen e tyre normale.

3. CSIRT Sektorial, në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të sektorit përkatës:

a. Suporton operatorin e infrastrukturës së sektorit përkatës për të rikthyer shërbimet dhe të dhënat në gjendjen e tyre normale dhe orienton përdorimin e mjeteve dhe teknikave për të përjashtuar kërcënimet dhe për të riparuar dëmet e shkaktuara si dhe izolimin e pajisjeve fundore dhe sistemeve të prekura për të parandaluar dëmtime të mëtejshme.

4. CSIRT pranë operatorit në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të operatorit përkatës:

a. Punon për të rikthyer shërbimet dhe të dhënat në gjendjen e tyre normale duke përdorur mjete dhe teknika për të përjashtuar kërcënimet dhe për të riparuar dëmet e shkaktuara si dhe izolimin e pajisjeve fundore dhe sistemeve të prekura për të parandaluar dëmtime të mëtejshme
b. Punon për pastrimin e komponentëve të incidentit në sistemet e prekura, si fshirja e skedarëve keqdashës, çaktivizim i llogarisë së përdoruesit, etj, sipas kategorisë së incidentit.
c. Punon për të eliminuar kërcënimet kibernetike duke çaktivizuar sistemet e infektuara, duke skanuar për malware dhe duke adresuar vulnerabilitetet;
ç. Punon për rikthimin në gjendjen e tyre para kompromentimit duke përdorur kopje rezervë të pastra. Gjithashtu i kërkon operatorit të bëjë monitorim për aktivitete të dyshimta dhe zbatohen arnimet e sigurisë për të adresuar dobësitë që shkaktuan ndërhyrjen;
d. Punon për të adresuar vulnerabilitetet që shkaktuan ndërhyrjen në sistemet e rikthyera;
dh. Monitoruar sistemet e rikthyera për aktivitet të dyshimtë.

5. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale në cilësinë e institucionit përgjegjës për hartimin e politikave për mbrojtjen e të dhënave personale të individëve, monitoron zbatimin e legjislacionit përkatës në rastin e incidenteve dhe krizës kibernetike:

a. Trajton, kontrollon, dhe monitoron zbatimin e legjislacionit ne fuqi mbi mbrojtjen e të dhënave personale.