Strategjia Kombëtare për Sigurinë Kibernetike 2023-2027

Shtator 2023

Përmbajtja

1 LISTA E SHKURTESAVE DHE PËRKUFIZIMEVE

1.1 Shkurtesat

CERT	Ekipi për Reagim ndaj Emergjencave Kompjuterike
CSIRT	Ekipi për Reagim ndaj Incidenteve të Sigurisë Kompjuterike
IKK	Infrastruktura Kritike Kombëtare
IKI	Infrastruktura Kritike e Informacionit
ASK	Agjencia për Siguri Kibernetike
KE	Këshilli i Evropës
MNSB	Masat e Ndërtimit të Besimit dhe Siguris
ENISA	Agjencia Evropiane e Sigurisë të Rrjetit dhe Informacionit
BE	Bashkimi Evropian
EUROPOL	Zyra Evropiane e Policisë
INTERPOL	Organizata Ndërkombëtare e Policisë Kriminale
TIK	Teknologjia e Informacionit dhe Komunikimit
IOCTA	Vlerësimi i Kërcënimeve të Krimit të Organizuar në Internet
IP	Protokolli i internetit
ISP	Ofruesi i Shërbimit të Internetit
TI	Teknologjia e Informacionit
PK	Policia e Kosovës
ITU	Unioni Ndërkombëtar i Telekomunikacionit
KShSK	Këshilli Shtetëror për Siguri Kibernetike
MPB	Ministria e Punëve të Brendshme
EKPÇ	Ekipi Kombëtar i Përgjigjes të Çastit
OECD	Organizata për Bashkëpunim dhe Zhvillim Ekonomik
Direktiva NIS	Direktiva e BE-së për Sigurinë e Rrjetit dhe Informacionit
OSHE	Operatorët e Shërbimeve Esenciale
DNS	Sistemi i emrave të domeinit
ZK	Zyra e Kryeministrit
PPPZK	Partneriteti Publik Privat Zyra e Kryeministrit
MEVGJ	Material Eksplicit i Vetë-Gjeneruar
PPP	Partneriteti Publik Privat
TLD	Domeni i Nivelit të Lartë
MEVGJ	Material Eksplicit i Vetë-Gjeneruar
OSBE	Organizata për Siguri dhe Bashkëpunim në Evropë
UNDP	Programi i Kombeve të Bashkuara për Zhvillim
NATO	Organizata e Traktatit të Atlantikut të Veriut
GEQ (GGE)	Grupi i Experteve Qeveritar ne OKB

ICANN Korporata e Internetit për Caktimin e Emrave dhe Numrave

1.2 Përkufizimet

Lista e mëposhtme përfshin shumë nga termat më të zakonshëm të përdorur në përcaktimin, përshkrimin dhe eksplorimin e sigurisë kibernetike dhe çështjet e ndërlidhura me të në kontekstin e këtij dokumenti. Lista duhet të përdoret për referencë, por nuk i zëvendëson përkufizimet dhe përshkrimet e vendosura në legjislacionin dhe strategjitë e aprovuar.

1.2.1. Bug- Bounty

Kërkon cenueshmeritë e softuerit të bërë nga personat që nuk janë të lidhur me zhvilluesin e softuerit, zakonisht me pëlqimin e përgjithshëm të zhvilluesit.

1.2.2. Funksioni vital i shoqërisë

Veprimtaritë, mallrat dhe shërbimet që janë jetike për funksionimin e përgjithshëm të shoqërisë.

1.2.3. Infrastruktura kritike

Infrastruktura, duke përfshirë objektet, sistemet, proceset, rrjetet, teknologjitë, asetet dhe shërbimet - të nevojshme për të ruajtur ose rivendosur funksionet jetike të shoqërisë.

1.2.4. Infrastruktura kritike e TIK

Nëngrupi i infrastrukturës kritike e cila përfshin infrastrukturën digjitale të nevojshme për të ruajtur ose rivendosur funksionet jetike të shoqërisë.

1.2.5. Infrastruktura Kritike Kombëtare

Një aset, sistem apo pjesë të saj të domosdoshme për mirëmbajtjen e funksioneve jetike dhe sociale, shëndetit, sigurisë, mirëqenies ekonomike ose shoqërore të njerëzve, dhe çrregullimi ose shkatërrimi i së cilës do të kishte një ndikim të konsiderueshëm në Republikën e Kosovës.

1.2.6. Sistemet kritike te TIK-ut për shoqërinë

Sistemet e TIK ku ndërprerjet e mëdha rezultojnë në sfida të rëndësishme për shoqërinë në tërësi. Mosdisponueshmëria dhe funksionimi i paqëndrueshëm i sistemeve të TIK-ut mund të ketë pasoja të mëdha për shoqërinë dhe për mirëmbajtjen e proceseve kritike për shoqërinë.

1.2.7. Infrastruktura Kritike e Informacionit (IKI)

a) Entiteti që ofron një shërbim i cili është esencial për mirëmbajtjen e aktiviteteve kritike dhe/ose ekonomike të shoqërisë,
b) Ofrimi i atij shërbimi varet nga rrjeti dhe sistemet e informacionit dhe
c) Një incident do të kishte efekt domethënës në ofrimin e atij shërbimi.

1.2.8. Siguria Kibernetike

Nënkupton aktivitetet e nevojshme për të mbrojtur sistemet e rrjetit dhe informacionit, përdoruesit e këtyre sistemeve dhe personave të tjerë të prekur nga incidenti kibernetik.

1.2.9. Krimi kibernetik

Nënkupton veprimtari kriminale (si mashtrimi, vjedhja ose shpërndarja e pornografisë së fëmijëve) e kryer duke përdorur një kompjuter veçanërisht për të hyrë, transmetuar ose manipuluar në mënyrë të paligjshme të dhëna.

1.2.10. Sistemi kompjuterik

Nënkupton një pajisje apo grup pajisjesh të ndërlidhura, një ose më shumë prej të cilave, në bazë të një programi, kryejnë përpunim automatik të të dhënave;

1.2.11. Të dhënat kompjuterike

Nënkupton një paraqitje të fakteve, informatave ose koncepteve në një formë të përshtatshme për përpunim në një sistem informacioni, përfshirë një program të përshtatshëm i cili mundëson që një sistem informacioni të kryejë një funksion. Të dhënat kompjuterike përfshijnë por nuk kufizohen në dokumente të shkruara, fotografi, audio dhe video materiale, programet softuerike dhe materialet tjera që ruhen në formë digjitale;

1.2.12. Shkelja e të dhënave

Shpalosje e paautorizuar e informatave që rrezikon sigurinë, konfidencialitetin ose integritetin e informatës personale të identifikueshme.

1.2.13. Mohimi (pamundësimi) i shpërndarë i shërbimit (DDoS)

Një lloj sulmi i mohimit të shërbimit në të cilin një sulmues përdor një kod me qëllim të keq të instaluar në kompjuterë të ndryshëm për të sulmuar një objektiv të vetëm.

1.2.14. Ndërvarësia

Varësia reciproke e plotë ose e pjesshme e disa mallrave ose shërbimeve.

1.2.15. Siguria e TI-së

Përfshin disponueshmërinë, integritetin, verifikimin dhe konfidencialitetin e informacionit në përdorimin e teknologjisë së informacionit. Për këtë arsye,

- ‘Disponueshmëria’ nënkupton situatën në të cilën sigurohet përdorueshmëria e nevojshme e informacionit si sisteme dhe përbërës të TI-së,
- 'Integriteti' i referohet përjashtimit të modifikimeve të paautorizuara dhe të ndaluara të informacionit si të sistemeve dhe komponentëve të TI-së;
- 'Verifikueshmëria' nënkupton situatën në të cilën veçoritë e kërkuara ose të premtuara të informacionit ose të procesit të transferimit mund të verifikohen nga përdoruesit dhe vis-a-vis palëve të treta;

- ‘Konfidencialiteti’ i referohet përjashtimit të marrjes ose sigurimit të paautorizuar të informacionit.

1.2.16. Qëndrueshmëria

Nënkupton aftësin për të **parandaluar, rezistuar, zbutur, amortizuar, akomoduar dhe rikthim** nga një incident i cili ndërpret ose ka potencialin të ndërpret veprimet e një entiteti kritik.

1.2.17. Shërbimi esencial

(a) Një shërbim i cili është esencial për mirëmbajtjen e aktiviteteve kritike dhe/ose ekonomike të shoqërisë,
(b) Ofrimi i atij shërbimi varet nga rrjeti dhe sistemet e informacionit, dhe
(c) Një incident do të kishte efekt domethënës në ofrimin e atij shërbimi.

1.2.18. Hakeri

Kushdo që përdor kompjuterë dhe internet për të hyrë në kompjuterë dhe serverë pa autorizim.

1.2.19. Softuer Dashakeq ose Malware

Nënkupton softuer me qëllim të keq i krijuar për të depërtuar ose dëmtuar një sistem kompjuterik, pa pëlqimin e pronarit. Format e zakonshme të *Malware* përfshijnë viruset kompjuterike, krimbët, trojanët, *spywarët, aduerët, etj.*

1.2.20. Ransomware

Nënkupton softuer i cili ju mohon qasjen në dosjet tuaja derisa të paguani një shpërblim të caktuar.

***1.2.21.* Spear Phishing**

Nënkupton përdorimin e postes elektronike mashtruese për të bindur personat brenda një organizate të shpalosin emrat e përdoruesve dhe/ose fjalëkalimet e tyre. Ndryshe nga phishing, i cili përfshin postime masive, spear phisihing është në shkallë të vogël dhe i shënjestruar mirë.

1.2.22. Ofrues i shërbimit

i. Secili entitet publik ose privat i cili ju ofron përdoruesve të shërbimit të tij mundësinë për të komunikuar me anë të një sistemi kompjuterik, dhe
ii. Secili entitet tjetër i cili përpunon ose ruan të dhëna kompjuterike në emër të këtij shërbimi të komunikimit ose përdoruesve të këtij shërbimi.

1.2.23. Trafiku i të dhënave

Nënkupton çdo lloj të dhënash kompjuterike që janë pjesë e një komunikimi nëpërmjet një sistemi kompjuterik, të prodhuara nga një sistem kompjuterik që formojnë një pjesë në zinxhirin e komunikimit, që tregojnë origjinën e komunikimit, destinacionin, rrugën, kohën, datën, madhësinë, kohëzgjatjen, apo llojin e shërbimit përkatës;

1.2.24. Sistem informacioni

Nënkupton një pajisje ose grup pajisjesh të ndërlidhura, ku një ose më shumë prej tyre në bazë të një programi, përpunojnë në mënyrë automatike të dhëna kompjuterike, po ashtu të dhëna kompjuterike të ruajtura, përpunuara, të marra ose transmetuara nga ajo pajisje ose grup i pajisjeve për qëllime të operimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre;

1.2.25. Rrjeti i komunikimeve elektronike

Nënkupton sistemin e transmetimit dhe nëse ekzistojnë, pajisjet e komutimit ose rutinimit dhe resurset tjera, duke përfshirë elementet e rrjetit që nuk janë aktive, të cilat lejojnë përcjelljen e sinjaleve nëpërmjet përcjellësve, radios, mjeteve optike ose mjeteve të tjera elektromagnetike, duke përfshirë rrjetet satelitore, rrjetet fikse (me komutim të qarqeve ose me komutim të paketave, përfshirë internetin), rrjetet mobile tokësore, sistemet e kabllove elektrike në raste kur ato përdoren për transmetimin e sinjaleve, rrjetet e përdorura për transmetimet radiotelevizive dhe të televizionit kabllor, pavarësisht nga tipi i informacionit të bartur;

1.2.26. Sistemi i rrjetit dhe informacionit

1.2.26.1. Një rrjet komunikimi elektronik, siç definohet në paragrafin 1.2.25;

1.2.26.2. Çdo sistem informacioni, siç definohet në paragrafin 1..2.24;

1.2.26.3. Të dhënat digjitale të ruajtura, përpunuara, pranuara ose transmetuara nga elementet e mbuluara në pragrafin 1.2.26.1. dhe 1.2.26.2. për qëllimet e operimit, përdorimit, mbrojtjes dhe mirëmbajtjes së tyre;

1.2.27. Siguria e sistemeve të rrjetit dhe informacionit'

Nënkupton aftësinë e sistemeve të rrjetit dhe informacionit për të rezistuar, në një nivel të caktuar besueshmërie, çdo veprimi që komprometon disponueshmërinë, origjinalitetin, integritetin ose konfidencialitetin e të dhënave të ruajtura ose të transmetuara ose të përpunuara ose shërbimet përkatëse të ofruara nga, apo të qasshme nëpërmjet këtyre sistemeve të rrjetit dhe informacionit;

1.2.28. Operatori i shërbimeve esenciale

Është entitet që i plotëson kriteret në vijim:

- Entiteti që ofron një shërbim i cili është esencial për mirëmbajtjen e aktiviteteve kritike shoqërore dhe/ose ekonomike,
- Ofrimi i atij shërbimi varet nga rrjeti dhe sistemet e informacionit, dhe

- Një incident do të kishte efekte të rëndësishme në ofrimin e atij shërbimi.

1.2.29. Ofruesi i shërbimit digjital

Çdo person juridik që ofron një shërbim digjital.

1.2.30. Pika e shkëmbimit të internetit (IXP)

Një strukturë e rrjetit që mundëson ndërlidhjen e më shumë se dy sistemeve autonome të pavarura. ISP-të lokale lidhen me *IXP* për të shkëmbyer trafikun në vend që të përdorin ofruesin në rrjedhën e sipërme.

1.2.31. Sistemi i emrave të domenit (*DNS*)

Një sistem hierarkik i emërtimit i shpërndarë në një rrjet që referon pyetje për emrat e domeneve dhe ndërlidh ato me IP adresat e caktuara.

1.2.32. Ofrues i shërbimit DNS

Një subjekt i cili ofron shërbime DNS në internet.

1.2.33. Domeni i nivelit të lartë (TLD)

Një subjekt i cili administron dhe operon regjistrimin e emrave të domeneve të internetit nën një domen specifik të nivelit të lartë (TLD).

1.2.34. Tregu online

Një shëërbim digjital që i mundëson ëkonsumatorëve dhe tregtarëve, të shesin në internet ose të lidhin kontrata të ëshërbimit në ueb-faqen e tregut online ose ënë ueb-faqen e ënjë tregtari ëqë ëpërdor ëshërbime kompjuterike ëtë ofruara nga tregu online.

1.2.35. Konsumator

Çdo person fizik që vepron ëpër qëllime që janë jashtë tregtisë, biznesit, zanatit ose profesionit të tij;

1.2.36. Tregtar

Çdo person fizik ose juridik pavarësisht nëse është në pronësi private apo publike, i cili vepron, duke përfshirë çdo person që vepron në dobi të tij apo në emër të tij, për qëllime që lidhen me tregtinë, biznesin, zanatin ose profesionin e tij;

1.2.37. Motor kërkimi në internet

Nënkupton një shërbim digjital që i mundëson përdoruesve të kryejnë kërkime, në parim, në të gjitha uebfaqet në një gjuhë të caktuar, në bazë të një kërkese për çfarëdo teme në formën e një fjale, fraze ose të dhëne tjetër, dhe kthen vegëza në të cilat mund të gjenden

informatat lidhur me përmbajtjen e kërkuar;

1.2.38. Shërbimi i cloud computing

Nënkupton një shërbim digjital që mundëson qasje në një pako të shkallëzuar dhe elastike të burimeve/resurseve kompjuterike të shpërndara. Burimet kompjuterike përfshijnë burime të tilla si rrjetet, serverët ose infrastruktura tjetër, hapësira ruajtëse, aplikacionet dhe shërbimet;

1.2.39. Internet i gjërave (IoT)

Një sistem i pajisjeve kompjuterike të ndërlidhura, pajisjeve mekanike dhe digjitale, objekteve, kafshëve ose njerëzve të cilët pajisen me identifikues unik (*UID*) dhe aftësinë për të transferuar të dhëna përmes një rrjeti, pa kërkuar ndërveprim njeri me njeriun ose njeri me kompjuter.

1.2.40. Qytet i mençur

Një emërtim i dhënë një qyteti që përfshin teknologjitë e informacionit dhe komunikimit për të përmirësuar cilësinë dhe performancën e shërbimeve urbane si energjia, transporti dhe shërbimet komunale, në mënyrë që të zvogëlojë konsumin e burimeve, humbjeve dhe kostove të përgjithshme.

2 HYRJE

Strategjia kombëtare e sigurisë kibernetike e Republika së Kosovës paraqet një plan të drejtimeve, qasjeve dhe objektivave strategjike të miratuara nga Qeveria e Kosovës që synojnë të përmirësojnë sigurinë dhe qëndrueshmërinë e infrastrukturës dhe shërbimeve kombëtare. Dokumenti i strategjisë ndihmon në krijimin e një qasjeje ndaj sigurisë kibernetike të rrënjosur në objektivat dhe prioritetet kombëtare të cilat duhet të arrihen brenda një kornize kohore specifike.

Në Kosovë, përdorimi i teknologjisë së informacionit dhe komunikimit është zgjeruar me shpejtësi prej vitit 2000, ndërsa tanimë TIK-u luan rol të rëndësishëm në të gjitha aspektet e jetës sonë. Sipas statistikave botërore të internetit, penetrimi i internetit në Kosovë është 90.4 % më 1,693,942 përdorues te internetit[1]. Ky trend i shpërndarjes së internetit dhe përdorimit të pajisjeve të TIK është i krahasueshëm më vendet e zhvilluara të BE-së, derisa edhe sjelljet e qytetarëve të Kosovës në internet duket të jenë të ngjashme me trendet globale. Shumica e institucioneve të Kosovës kanë zhvendosur punët e tyre të përditshme në internet, përfshirë, organizatat që ofrojnë shërbime në sektorët kritikë të infrastrukturës si energjia, uji, shëndetësia, transporti dhe komunikimi. Këto sisteme përmirësojnë cilësinë dhe shpejtësinë e shërbimeve që ofrohen, duke u ndihmuar kështu organizatave që të punojnë në mënyrë më produktive, duke kontribuar kështu drejt përmirësimit të standardeve të jetesës.

Analizat e përsëritura tregojnë se jeta e qytetarëve të Kosovës është kryesisht e varur nga ajo që ne tani mund ta quajmë teknologji tradicionale, por edhe emergjente, duke siguruar shkëmbime të rëndësishme të përditshme si komunikimi social, transaksionet me sektorin privat, përpjekjet akademike dhe ndoshta më e rëndësishme - shkëmbimet me sektorin publik në pranimin e shërbimeve publike. Për shembull, një anketim digjital i realizuar nga UNDP në Kosovë në vitin 2021 më 2,400 familje mbi qasjen, përdorimin dhe përballueshmërinë e mjeteve digjitale, shërbimet që kanë të bëjnë me ndryshimin e sjelljes, marrjen e shërbimeve publike, etj. paraqet se Kosova shfaq **qasje të gjerë** në internet dhe pronësi të pajisjeve të teknologjisë të informacionit dhe komunikimit siç janë kompjuterët dhe telefonat celularë në mesin e popullatës, **me mbi 99.7% të familjeve** të raportuara **që kanë qasje në internet[2]**.

Një hapësirë kibernetike e sigurt është jetike për zhvillimin e shërbimeve të TIK-ut dhe të internetit. Nga ana tjetër, kërkesa për internet dhe lidhje kompjuterike na shpie në integrimin e teknologjisë kompjuterike në produkte që zakonisht kanë funksionuar pa të, të tilla si makinat dhe ndërtesat. Përveç kësaj, ne shohim aplikimet e tij në ofertën e shërbimeve publike, ndërsa zgjidhjet digjitale si e-qeveria, e-tregtia, e-arsimi, e-shëndetësia dhe e-mjedisi varen nga përdorimi i TIK-

[1] https://www.internetworldstats.com/europa2.htm#kv

[2] Vizualizuesi Digjital i të Dhënave të Anketimit të Amvisërive (DHS) është në dispozicion në: www.undp.org/kosovo/digital

ut. Përfundimisht, edhe shërbimet esenciale si furnizimi me ujë dhe energji elektrike mbështeten gjithnjë e më shumë në TIK[3] këtyre ditëve.

Tërësia e këtyre veprimeve fuqizon vlerën e angazhimit të publikut me teknologjinë dhe internetin, por në të njëjtën kohë, ato mbeten të lidhura në mënyrë negative me ekspozimin e publikut ndaj llojeve të kanosjeve të cilat do të ishin të pamundura në një realitet analog. Prandaj, mundësitë të cilat rrjedhin nga ndërveprimi i qytetarëve të Kosovës me teknologjinë dhe internetin përputhen me atë se sa mirë i pranojmë dhe trajtojmë sfidat dhe dobësitë në fushën e sigurisë kibernetike. Së fundi, kjo e pozicionon sigurinë kibernetike si parakusht për një transformim digjital të përshpejtuar në Kosovë, i cili është gjithashtu në përputhje me Agjendën Digjitale 2030 të Kosovës. Kjo strategji kombëtare kontribuon në realizimin e objektivave të Agjendës Digjitale.

2.1 Qëllimi

Qëllimi i këtij dokumenti strategjik është që të përcaktoj objektiva e avancimit të kapaciteteve të përgjithshme dhe specifike të institucioneve të Republikës së Kosovës në fushën e sigurisë kibernetike për vitet vijuese. Për më tepër, ky dokument paraqet vizionin e Qeverisë së Kosovës për sigurinë kibernetike dhe përcakton planin përkatës të veprimit.

2.2 Vizioni

”Republika e Kosovës do të krijoj mjedis online të sigurt dhe të qëndrueshëm për të gjithë qytetarët, bizneset dhe qeverinë, duke punuar në zvogëlimin e dobësive dhe zhvillimin e aftësive dhe kapaciteteve për të trajtuar çështjet e sigurisë kibernetike duke parandaluar dhe minimizuar dëmet”.

[3]:Një Kornizë Kombëtare e Përgjithshme për Mbrojtjen e Infrastrukturës të Informacionit Kritik, 2007, është në dispozicion në www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

3. METODOLOGJIA

Strategjia Shtetërore për Sigurinë Kibernetike është hartuar duke u bazuar në vlerësimet dhe analizat e institucioneve të Kosovës, agjencive të zbatimit të ligjit, nevojave të sektorit privat, organizatave vendore dhe ndërkombëtare, trendeve globale, si dhe praktikave dhe politikave të BE-së. Në këtë kontekst, strategjia është në harmoni të plotë me udhëzimet e ENISA-s dhe praktikat e strategjive të shteteve anëtarë të BE-së.

Metodologjia e përdorur gjatë punës për hartimin e strategjisë kombëtare për siguri kibernetike është paraqitur në skemën e mëposhtme:

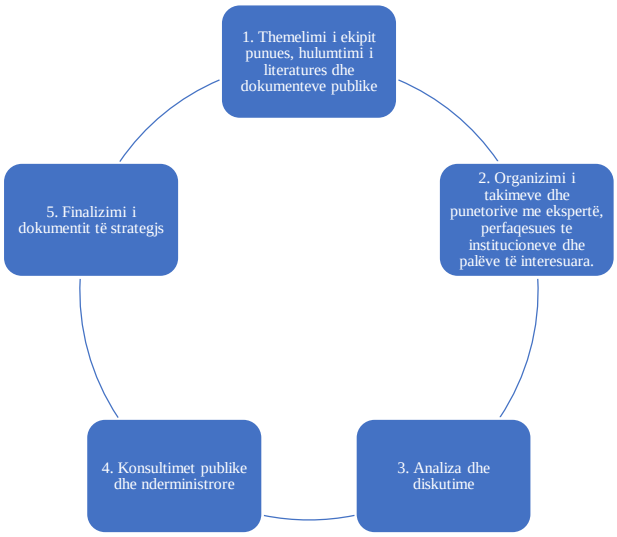

Figure 1 - Metodologjia e përdorur gjatë punës për hartimin e strategjisë

1. **Themelimi i ekipit punues, hulumtimi i literatures dhe dokumenteve publike** - Më vendimin nr. 973/2021 të datës 30.09.2021, Sekretarja e përgjithshme e MPB-së ka themeluar ekipin punues për hartimin e strategjisë për siguri kibernetike dhe planin e veprimit. Në përbërje të ekipit punues kanë marrë pjesë përfaqësues nga institucionet publike, ekspertët ndërkombëtarë, shoqatat profesionale, sektori privat, shoqëria civile dhe organizatat partnere ndërkombëtarë. Ekipi punues ka për detyrë hartimin e strategjisë për sigurinë kiberneitke dhe planin e veprimit në nivel shtetëror.

2. **Organizimi i takimeve dhe punëtorive me ekspertë, perfaqësues të institucioneve dhe palëve të interesuara** – Për hartimin e strategjisë kombëtare për siguri kibernetike janë mbajtur takime dhe disa punëtori me përfaqësues të institucioneve publike, ekspertë vendorë dhe ndërkombëtarë, përfaqësues të organizatave ndërkombëtare partnere dhe shoqërisë civile. Punëtoria e parë është mbajtur më datat 20 dhe 22 dhjetor 2021, në të cilën është raportuar për mënyrën e realizimit të strategjisë së parë të sigurisë kibernetike dhe planit të veprimit 2016 – 2019. Njëkohësisht është përcaktuar mënyra e organizimit të

punës për hartimin e strategjisë së re. Më datat 17 – 18 mars 2022 është mbajtur punëtoria e dytë në të cilen janë diskutuar objektivat strategjike dhe specifike për strategjinë e re. Më datë 23.12.2022 është mbajtur punëtoria e tretë ku janë diskutar aktivitetet e planit të veprimit.

3. **Analiza dhe diskutime -** Është analizuar literatura teorike dhe empirike në fushën e sigurisë kibernetike dhe janë përdorur si materiale bazë burimet parësore dhe dytësore si: analizat dhe vlerësimet e riskut nga institucionet shtetërore, zbatimi i strategjisë së parë të sigurisë kibernetike, publikimet e ndryshme të organizatave vendore dhe ndërkombëtare, mendimet dhe vlerësimet e ekspertëve, udhëzimet e ENISA-së dhe dokumentet tjera relevante.

4. **Konsultimet publike dhe ndërministrore–** Nga data 13.03.2023 deri më 03.04.2023 dokumenti i strategjisë është vendosur në konsultime publike. Gjatë kësaj periudhe janë pranuar komente nga institucionet vendore dhe ndërkombëtare.

5. **Finalizimi i strategjisë –** Pas analizes së komentëve është finalizuar dokumenti i strategjisë dhe planit të veprimit.

4. PARIMET UDHËZUESE

Në vijim do të paraqiten parimet udhëzuese për qeverinë, bizneset dhe komunitetin.

4.1. Parimet udhëzuese për qeverinë

Derisa ky dokument i përcakton kryesisht parametrat për një plan të veprimit funksional dhe hapat e ardhshëm drejt një hapësire të sigurt kibernetike, institucionet duhet të respektojnë parimet e mëposhtme për të maksimizuar ndikimin e një strategjie të unifikuar*:*

1. Të garantoj që korniza ligjore dhe metodat për identifikimin e IKI janë vendosur dhe ofrojnë udhëzime për t'u siguruar që entitetet e IKI janë identifikuar dhe kanë kapacitetet e nevojshme për t'i reduktuar rreziqet kibernetike.

2. Të krijoj një kuadër të qartë bashkëpunimi me vendet e tjera për të parandaluar, zbuluar, alarmuar dhe trajtuar incidentet kibernetike.

3. Të promovoj bashkëpunimin ndërkombëtar mbi sigurinë kibernetike dhe bashkëpunimin mbi luftimin e krimit kibernetikë dhe zhvillimin e diplomacisë kibernetike.

4. Të punoj për të mbrojtur IKK, shërbimet esenciale dhe komunitetin. Si e tillë, përpiqet të mbrojë si në vijim:

- Mbron të dhënat, sistemet dhe rrjetet e qeverisë;
- Krijon mekanizma, udhëzime dhe forume për t'i mbështetur bizneset për t'i përmbushur standardet e sigurisë kibernetike;
- Promovon një ekosistem të startup-eve të sigurisë kibernetike dhe tërheq investime;
- Zhvillon dhe mirëmbanë ngritjen e kapaciteteve për sigurinë kibernetike si trajnime për zyrtarët dhe një planprogram specifik arsimor mbi sigurinë kibernetike për shkolla dhe universitete;

5. Të siguroj që Kosova të vazhdojë qasjen e saj kombëtare për zhvillimin e një kornize ligjore për sigurinë kibernetike për ta bërë hapësirën kibernetike më të sigurt dhe për të ndihmuar në luftimin e krimit kibernetik.

6. Institucionet, përmes politikave dhe procedurave të tyre administrative, sigurojnë që të gjitha qasjet ndaj sigurisë kibernetike mbeten të orientuara tek njerëzit në qendër dhe gjithëpërfshirëse për shoqërinë.

7. Te siguroj qe Kosova do te zhvilloj kapacitetet e saj per siguri kibernetike ne harmoni me normat vullnetare te GEQ (GGE).

4.2. Parimet udhëzuese për sektorin privat

Në vazhdim, janë renditur disa parime udhëzuese të cilat duhet të adaptohen nga sektori privat në mënyrë që të ekzistojë një qasje përparuese mbarëkombëtare ndaj sigurisë kibernetike:

1. Entitetet e sektorit privat duhet të përmirësojnë sigurinë minimale për tërë IKK-të.

2. Kompanitë private që zotërojnë IKI, duhet t'i kryejnë vlerësimet periodike të rrezikut në mënyrë që t'i identifikojnë cenueshmëritë dhe varësitë e ndërsjella ndërmjet infrastrukturave. Ata gjithashtu duhet të krijojnë programe sigurie të bazuara në mekanizma përmirësimi të vazhdueshëm për të siguruar që masat parandaluese janë zbatuar në mënyrë efikase dhe efektive. Kjo do të ndihmojë në sigurimin e plotë të zinxhirit të vlerës digjitale.

3. Entitetet e sektorit privat duhet te ushtrojn kujdesin e duhur ne mbrojtje te sistemeve te tyre te rrjetit dhe informacionit si dhe te jene reaguesit e parë në rast të incidenteve kibernetike.

4. Bizneset dhe agjencitë e tjera duhet të investojnë në ndërtimin e një fuqie punëtore të aftë për sigurinë kibernetike.

5. Bashkëpunimi ndërmjet sektorit privat dhe Qeverisë së Kosovës duhet të bazohet në parime si besimi reciprok, transparenca, ndarja e informacionit për kërcënimet dhe incidentet kibernetike, si dhe ndarja e ekspertizës.

4.3. Parimet udhëzuese për komunitetin

Së fundi, një hapësirë e sigurt kibernetike nuk mund të ekzistojë pa mirëkuptimin dhe bashkëpunimin e komunitetit. Si të tilla, parimet e mëposhtme duhet të vendosen në vetëdijen e gjithë komunitetit dhe duhet të respektohen në mënyrë që të krijohet një hapësirë e sigurt në internet:

1. Çdo person ka përgjegjësinë të sigurojë që kompjuteri i tij ose i saj, telefoni celular ose çdo infrastrukturë e TIK-ut në dispozicion të tij ose të saj të jenë të përditësuara dhe të ketë mbrojtje ndaj malware.

2. Të gjithë qytetarët kanë përgjegjësi që të informohen kur vendosin për blerjet në internet dhe të kërkojnë më shumë informacione kur nuk janë të sigurt.
3. Të gjithë qytetarët duhet t'i raportojnë krimet kibernetike në të njëjtën mënyrë siç do të trajtonin secilin krim tjetër të përcaktuar brenda kornizës ligjore të Qeverisë të Kosovës.

5. SFIDAT, RREZIQET, KËRCËNIMET NDAJ SIGURISË SË HAPËSIRËS KIBERNETIKE NË KOSOVË

Kuptimi i qartë i problematikës që ndërlidhet me sigurin e hapësirës kibernetike në Republikën e Kosovës nga te gjitha palët, është thelbësore për t'u mundësuar bashkëpunimi dhe koordinimi efektiv në mes të palëve që kanë mandat dhe përgjegjësi në këtë fushë.

Mbrojtja e IKI është thelbësore për Qeverinë e Republikës së Kosovës, veçanërisht pasi sulmet e suksesshme kibernetike ndaj kësaj infrastrukture, do të kishin ndikim të konsiderueshme në vend. Këto ndikime mund të përfshijnë destabilizimin e ekonomisë dhe dëmtimet e reputacionit të bizneseve dhe individëve. Prandaj, është me rëndësi jetike që Republika e Kosovës t'i kushtojë rëndësi mbrojtjes së IKI, të cilat janë thelbësore për garantimin e ofrimit të shërbimeve esenciale.

Mbrojtja e IKI, kërkon bashkëpunimin e të gjithë akterëve relevantë, përfshirë institucionet publike dhe private që zotërojnë ose operojnë më IKI, e cila mbështet funksionimin e duhur të shoqërisë. Në këtë kuptim, aktivitetet duhet të adresohen tek të gjithë akterët relevantë për të identifikuar dhe kuptuar dobësitë dhe nivelet e sigurisë kibernetike të IKI në përgjithësi. Aktivitetet dhe veprimet do të fokusohen tek palët përkatëse për të vendosur masa që do të adresojnë kërcënimet dhe rreziqet e tanishme dhe të ardhshme kibernetike në IKI dhe të shtyjnë përmirësime atje ku është e nevojshme.

Derisa aftësitë kibernetike të kundërshtarëve po rriten, ato do të përbëjnë kërcënime në rritje për sigurinë, duke përfshirë infrastrukturën kritike, shëndetin, sigurinë publike, përparimin ekonomik dhe stabilitetin.[4]

Hapësira kibernetike mund të konsiderohet një terren i paqëndrueshëm. Aktivitetet kriminale po krijojnë vazhdimisht një kontekst konfliktuoz, ndërsa akterët shtetëror duhet t'i luftojnë aktivitetet kriminale të cilat kanosin sovranitetin qeveritar ose ekonomik. Në përputhje me këtë, ka evoluar një gamë e gjerë e sulmuesve, motiveve dhe teknikave, të cilat dëshmohen të jenë gjithnjë e më kërcënuese për Kosovën.

Për më tepër, duhet theksuar se hapësira kibernetike nuk paraqet vetëm një hapësirë virtuale, por edhe pjesë të komponentëve dhe sistemeve fizike me rëndësi shoqërore. Veprimet armiqësore në hapësirën kibernetike mund të rrezikojnë lehtësisht funksionimin e infrastrukturave kritike dhe shërbimeve esenciale, duke u bërë një kërcënim me përmasa kombëtare dhe për jetën. Kohët e fundit, objektet e IKK-së, qofshin ato termocentrale, objekte të transportit ajror apo forma të tjera të transportit publik, janë cak i sulmeve kibernetike gjithnjë e më shumë. Sulmet kibernetike mund të ndërpresin furnizimin me energji elektrike në spitale, shtëpi, shkolla dhe fabrika.

https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

Duke pasur parasysh se shoqëritë mbështeten aq shumë në furnizimin efikas me energji elektrike, ndërprerja për periudha të gjata kohore do të kishte gjithashtu ndikime të rënda për shërbime të tjera jetike.

5.1. Kërcënimet

Kërcënimet kibernetike tashmë po sfidojnë besimin e publikut në institucionet globale, qeverisje dhe madje edhe në norma.

Kërcënimet kibernetike vijnë nga mundësitë dhe qëllimet e keqbërësve që të fillojnë një sulm kibernetik ndaj sistemeve të TIK-ut.

Sulmet kibernetike mund të jenë të motivuara nga:

- **Hakmarrja:** Të kryera nga stafi brenda organizatës ose ish-të punësuar (të larguar nga puna);
- **Kurreshtja:** Të ashtuquajtur "script-kiddies" (të rinj që përdorin skripta të gatshme për sulme);
- **Përfitime monetare:** Të kryera nga individ apo grupe kriminale;
- **Spiunimi:** Sulmet kibernetike që kanë të bëjnë me ndërhyrjen e pavërejtur të një pale të tretë brenda sistemeve të TIK-ut, duke lexuar, ndryshuar, fshirë apo edhe shtuar informata. Ndërhyrjet e tilla mund të përdoren edhe për të keqpërdorur sistemet e sulmuara të komunikimit dhe të informacionit, dhe për të sulmuar sisteme të tjera;
- **Cenimi i sigurisë shtetërore:** Të kryera nga akterë të sponsorizuar nga shtetet tjera;
- **Terrorizmi kibernetik:** Ka të bëjë me përpjekje me shënjestra të nivelit të lartë, që bëhen për qëllime terroriste, i cili është një kërcënim në zhvillim e sipër dhe ka potencial të shkaktojë dëme të mëdha. Përderisa terrorizmi shpesh ndërlidhet me humbjen e jetës, nuk mund t'i anashkalojmë pasojat e rëndësishme si frikësimi apo shtytja që mund të shkaktohen nga terrorizmi kibernetik.

Grupet ekstremiste dhe radikale gjithnjë e më shumë përdorin hapësirën kibernetike për organizim dhe propagandë për të promovuar veprimtarinë e tyre, rekrutuar anëtarë të rinj dhe organizuar veprime terroriste, të cilat përbëjnë kërcënime ndaj sigurisë shtetërore të Republikës së Kosovës.

IKI është në vazhdimësi shënjestër e sulmeve kibernetike. Këto sulme veçanërisht shënjestrojnë caqe specifike të zgjedhura nga terroristët ose hakerët që kërkojnë informata të ndjeshme apo me qëllim që ta shkatërrojnë këtë infrastrukturë kritike.

5.2. Rreziqet

- Mungesa e legjislacionit për siguri kibernetike ku përcakton masat minimale të sigurisë për operatorët e shërbimeve esenciale dhe ofruesit e shërbime digjitale;
- Mungesa e vlerësimeve të rrezikut;
- Mungesa e listës së entiteteve të sektorëve që identifikohen si IKK, bazuar në ligjin për infrastruktur kritike.
- Mungesa e kapaciteteve profesionale-teknike për parandalim të sulmeve kibernetike.
- Mungesa e vetëdijes së qytetarëve për rreziqet në hapësirën kibernetike
- Mungesa e buxhetit të dedikuar në instirucionet e shtetit dhe sektorin privat për siguri kibernetike

5.3. Adresimi i krimit kibernetik

Krimi kibernetik mbetet një prej sfidave për institucionet e Republikës së Kosovës. Republika e Kosovës ka ndërmarrë hapa konkretë në krijimin e infrastrukturës ligjore për parandalimin dhe luftimin e të gjitha formave të krimit kibernetik, por ende mbesin shumë sfida, sidomos në kuptimin teknik të përballimit të suksesshëm me këtë formë të krimit.

Bashkëpunim i ngushtë ndërmjet agjencive të zbatimit të ligjit në gjithë botën është e domosdoshme, në mënyrë që të luftohet rritja e shpejtë e krimit kibernetik.

Rritja e konsiderueshme e numrit të shfrytëzuesve të internetit në vitet e fundit në Republikën e Kosovës ka sjellë me vete rrezikun e rritur të krimit dhe të sulmeve kibernetike. Disa veprimtari kriminale që kanë ndodhur janë të mjaftueshme për të theksuar dobësinë e rrjeteve kompjuterike që konsiderohen që janë në fazën e zhvillimit.

Sipas të dhënave në dispozicion, shënjestra kryesore e sulmeve kibernetike në Republiken e Kosovës ka qenë sistemi i rrjetit kompjuterik shtetëror, llogaritë e shfrytëzuesve, sistemi bankar, ueb faqet në internet dhe sektori privat.

Duhen përforcuar më tutje kapacitetet e agjencive të zbatimit të ligjit në luftimin e krimit kibernetik, si dhe në lidhje me mbrojtjen nga spiunimi dhe sabotimi. Po ashtu, nevojitet të avancohen mekanizmat institucional të zbatimit të ligjit për luftimin e krimeve kibernetike dhe forcimin e bashkëpunimit ndërkombëtar në shkëmbimin e informatave. Përveç kësaj, ka nevojë që të ofrohet zhvillim dhe trajnim profesional për zyrtarët e institucioneve të zbatimit të ligjit në mënyrë që të avancohen kapacitetet në ndjekje dhe zbulim të krimit kibernetik.

Krimi kibernetik kërkon reagim të specializuar të institucioneve. Agjencitë e zbatimit të ligjit duhet të jenë në gjendje të ndërmarrin veprime të koordinuara dhe të hetojnë veprat kundër vjedhjes dhe keqpërdorimit të të dhënave të sistemeve kompjuterike, veprat e kryera përmes kompjuterit, si dhe të siguroj dëshmitë elektronike të ndërlidhura me veprat penale.

5.4. Baraspeshimi i sigurisë dhe i privatësisë

Autoritetet publike dhe private në pajtim me Kushtetutën e Republikës së Kosovës, garantojnë respektimin e të drejtave dhe lirive themelore. Të drejtat themelore duhen garantuar edhe brenda hapësirës kibernetike. Rritja e sigurisë kibernetike mund të përmirësojë mbrojtjen e privatësisë dhe pronës së përdoruesve në hapësirën kibernetike.

Qeveria e Kosovës do të vazhdojë të ndërmarrë masat e nevojshme për mbrojtjen dhe garantimin e sigurisë kibernetike. Këto masa do të respektojnë privatësinë, të drejtat dhe liritë themelore, qasjen e lirë në informata dhe parimet tjera demokratike.

6. RRUGA PËRPARA

Të gjitha vendet synojnë një strategji kombëtare të informuar dhe funksionale të sigurisë kibernetike. Zhvillimi i një strategjie të tillë dhe veçanërisht zbatimi i saj me sukses nuk paraqet një detyrë të lehtë. Prandaj, prioritizimi strategjik është kyç për Republikën e Kosovës.

Qeveria e Kosovës synon që përmes 6 objektivave strategjike të realizoj vizionin e saj për hapësirë të sigurt kibernetike për qytetarë, biznese dhe institucionet publike.

7. OBJEKTIVAT E STRATEGJISË

Duke i shërbyer vizionit të përgjithshëm, duke i marrur parasysh konsideratat e renditura më sipër, strategjia do të punojë për t'i arritur gjashtë objektivat dhe synimet strategjike në vijim, brenda afatit kohor 2023-2027:

Objektivi Strategjik 1: Krijimi i kapaciteteve ligjore dhe institucionale të sigurisë kibernetike në nivel kombëtar.

Objektivi Strategjik 2: Promovimi i programeve vetëdijesuese për sigurinë kibernetike dhe një kulture të sigurisë kibernetike në Kosovë.

Objektivi Strategjik 3: Mbështetja në zhvillimin e sektorit privat në sigurinë kibernetike, PPP-së dhe shkëmbimit te informacionit ndër sektorial.

Objektivi Strategjik 4: Ndërtimi i bashkëpunimit të qëndrueshëm dhe të dobishëm kombëtar dhe ndërkombëtar në sigurinë kibernetike.

Objektivi Strategjik 5: Zhvillimi i kapaciteteve të qëndrueshme të sigurisë kibernetike për qeverinë dhe sektorin privat.

Objektivi Strategjik 6: Avancimi i aftësive hetimore dhe ushtarake të sigurisë kibernetike.

Në vazhdim, do të përshkruhet fushveprimtaria e secilit objektiv.

7.1. Objektivi Strategjik 1: Krijimi i kapaciteteve ligjore dhe institucionale të sigurisë kibernetike në nivel kombëtar.

Mbështetja e vazhdimësisë së shërbimeve esenciale në tërë Kosovën përballë sulmeve përçarëse apo të synuara, mbetet një obligim themelor i qeverisë. Ndërprerja e shërbimeve dhe funksioneve kritike shoqërore si energjia elektrike, uji, sistemet e komunikimit, komanda dhe kontrolli, transporti ajror mund të ketë një ndikim shkatërrues që mund të kërcënojë sigurinë kombëtare.

Në përgjithësi, çdo herë ekziston nevoja që të punohet më shumë në ngritjen e kapaciteteve të sigurisë së IKK-së. Disa akterë shtetërorë dhe jo-shtetërorë janë aq të përsosur sa që një sulm mund të jetë përtej aftësisë të një pronari të vetëm të rrjetit për ta trajtuar i vetëm, pavarësisht nga

madhësia, ekspertiza dhe përpjekjet më të mira. Prandaj, ky dokument përshkruan përgjigjet ndaj mjedisit të rrezikut në zhvillim të Kosovës me qëllim të ndërtimit të bazave të plota, aftësive të veçanta dhe partneriteteve që në përgjithësi do të përfitojnë të gjitha palët e interesuara, pavarësisht nëse janë nga sektori publik apo privat.

Si i tillë, dokumenti parashtron masat, rolet dhe përgjegjësitë e palëve përkatëse të interesit, në garantimin e sigurisë dhe qëndrueshmërisë së IKK të Kosovës, potencialin e krijimit të politikave për t'i paraparë kërcënimet e ardhshme dhe për të ndërmarrë veprime efektive në emergjencat e ardhshme.

7.1.1.Korniza rregullatore

Qeveria e Kosovës do të prezantojë një kornizë të përmirësuar rregullatore për t'i identifikuar dhe mbrojtur subjektet e IKI-së) nga të gjitha kanosjet, duke përfshirë këtu kërcënimet dinamike dhe potencialisht katastrofike nga sulmet kibernetike. Korniza do t'i përfshijë specifikimet mbi detyrimet e sigurisë për subjektet e IKK-së me kërkesa specifike për secilin sektor. Kjo është në përputhje me mbrojtjen kibernetike, fizike, stafin dhe zinxhirin e furnizimit në të gjithë sektorët, ndërkohë duke marrur në konsideratë se ekzistojnë dallime specifike për secilin sektor. Këto dallime mund të gjenden në burimet njerëzore dhe financiare, teknologjitë specifike, llojet e kërcënimeve, standardet ekzistuese dhe pjekurinë e subjekteve të ndryshme.

7.1.2.Udhëzimet

Të krijohen udhëzimet specifike për t'i identifikuar cenueshmëritë dhe varësitë ndërmjet infrastrukturave për të siguruar një qëndrim të duhur të sigurisë të zinxhirëve të furnizimit digjital. Udhëzimet do të përfshijnë një sërë të aktiviteteve të cilat synojnë të përmirësojnë të kuptuarit kolektiv të rrezikut brenda dhe ndërmjet sektorëve përkatës. Qeveria e Kosovës do të propozojë standarde minimale teknike për teknologji të sigurt dhe sigurinë e teknologjisë.

Institucionet e Kosovës do të nxjerrin udhëzime të sigurisë për prokurimin e TI-së, në përgjithësi. Për të gjitha IKK-të, do të ketë masa të zgjeruara të auditimit që përfshijnë zinxhirin e furnizimeve kritike.

7.1.3. Auditimet periodike

Për më tepër, do të ketë auditime periodike që do të zbatohen duke qenë ndër masat kyçe të cilat mundësojnë vlerësimin e efektivitetit të sistemeve të menaxhimit të sigurisë të zbatuara aktualisht, duke përfshirë përshtatshmërinë e masave mbrojtëse të prezantuara. Metodologjitë e auditimit duhet të marrin parasysh standardet e aplikueshme, praktikat e mira dhe specifikat e sektorëve përkatës. Përdorimi i plotë i kësaj qasjeje, siguron arritjen e krahasueshmërisë ndërmjet rezultateve të auditimit.

Një proces i suksesshëm i auditimit duhet të përmbajë elementët si më poshtë:

1. Mapimi i pajisjeve, mapimi i kritikalitetit, mapimi i qasshmërisë (Device mapping, criticality mapping, accessibility mapping);
2. Mapimi i kërcënimeve, duke përfshirë:
    i. Testimi i depërtimit;
    ii. Analiza e shkallës të defektit;
    iii. Kultura e sigurisë dhe analiza e arkitekturës të IKK-ve dhe komponentëve të zgjedhur tek prodhuesit;
    iv. Aftësitë në siguri së IKK-ve dhe kontraktorëve, dhe opcionet e kontraktimit.

Testimet periodike të cilat ofrojnë vlerësim real të qëndrueshmërisë së sistemit ndaj kërcënimeve, janë një tjetër masë e sigurisë. Rezultatet e këtyre testeve krijojnë bazën për verifikimin e masave që janë vendosur për mbrojtje. Për të shfrytëzuar kapacitetin publik në fushën e sigurisë kibernetike, do të praktikohet edhe testimi i bazuar në *bug-bounty*. Për të siguruar funksionimin e infrastrukturës kritike në sektorin e TIK-ut është jetike që të bëhet vlerësimi i rregullt i rreziqeve për funksionimin e infrastrukturës kritike, duke i planifikuar masat e duhura të mbrojtjes dhe duke përditësuar vlerësimin e rrezikut.

7.1.4. Qasjet për mbrojtje të infrastrukturës kritike

Përditësimet duhet të kryhen nga stafi i verifikuar dhe aprovuar. Të gjitha IKK-të duhet të kenë në strukturën e tyre CSIRT ose së paku një zyrtar të sigurisë së informacionit. Mund të themelohen CSIRT sektorial kombëtar për sektorët specifik të IKK, të cilët do të jenë përgjegjës për entitetet që janë pjesë e atij sektori në nivel kombëtar.

Infrastruktura kritike është gjithnjë e më shumë e ndërlidhur dhe e ndërvarur, e cila pa masa mbrojtëse të duhura krijon cenueshmëri dhe mund të shkaktojnë qëllimisht ose pa dashje përçarje të cilat mund të rezultojn me pasoja kaskadike për tërë ekonominë dhe sigurinë kombëtare të Kosovës. Incidentet e fundit në Kosovë, por edhe në mbarë botën, duke përfshirë ndikimet nga COVID-19, demonstrojnë se ato kërcënime mund të kenë ndikim të madh në funksionimin e subjekteve të infrastrukturës kritike.

Sulmet kibernetike mund të kenë pasoja të mëdha për funksionet vitale të shoqërisë dhe sistemet kritike të TI-së, dhe mund të konsiderohen si të ngjashme me një sulm të armatosur konvencional për këtë arsye në disa raste të caktuara mund të konsiderohen edhe si një sulm i armatosur. Një analizë e IKI-së duhet të bëhet për të mbështetur përgatitjen e hartës së IKK të Kosovës. Qëllimi është që shoqëria të jetë e pajisur dhe e përgatitur më mirë për të vazhduar funksionet vitale shoqërore në në raste të incidenteve të mëdha të sigurisë kibernetike. Sigurimi efektiv i këtyre sistemeve dhe i të dhënave brenda tyre është çështje e sigurisë dhe sovranitetit kombëtar. Qeveria e Kosovës do të konsolidojë infrastrukturën e saj të teknologjisë së informacionit për të rritur më tej sigurinë e saj.

Strategjia përfshin një sërë veprimesh strategjike për të forcuar sigurinë e funksioneve vitale të shoqërisë dhe për të siguruar që agjencitë qeveritare dhe bizneset të kenë një nivel të përshtatshëm të sigurisë. Disa nga masat kyçe përfshijnë:

1. Të gjitha agjencitë qeveritare duhet të operojnë në përputhje me standardet ndërkombëtare të cilat përcaktojnë praktikat më të mira për menaxhimin e sigurisë së informacionit.
2. Kërkesat e sigurisë për menaxhimin e sistemeve qeveritare të TIK të cilat janë kritike për shoqërinë do të forcohen për të siguruar që siguria brenda dhe rreth sistemeve të TIK-ut të ketë fokusin e duhur menaxherial.
3. Përfshirja dhe prioritizimi i sigurisë kibernetike dhe të informacionit në të gjitha nivelet e menaxhimit do të garantohet duke forcuar njohuritë, vetëdijësimin dhe sjelljen e menaxherëve të lartë në qeveri përmes kërkesave dhe pritshmërisë në rritje, si dhe iniciativave për shkathtësi të reja.

Zgjidhjet e përgjithshme teknike, si ato të bazuar në DNS, janë duke u krijuar për të fuqizuar sigurinë ndërmjet autoriteteve qeveritare. Implementimi i zgjidhjes së bazuar në DNS do të fuqizojë gatishmërinë e sigurisë teknike të operatorëve *t*ë IKK dhe do të përmirësojë kapacitetin e stafit të tyre teknik për të identifikuar dhe zbatuar zgjidhje efektive dhe të personalizuara.

Prandaj, Qeveria e Kosovës synon të ndërmarrë hapat e duhur për të siguruar që e gjithë IKI është identifikuar dhe mbrojtur siç duhet nga kërcënime të ndryshme. Kështu, një IKI e sigurt do të ndihmojë në arritjen e vazhdimësisë së ofrimit të shërbimeve esenciale dhe do të mbështesë sigurinë kombëtare, përparimin ekonomik dhe mirëqenien sociale të Kosovës.

Sulmet gjithashtu mund të jenë të drejtuara ndaj vlerave tona themelore dhe funksioneve demokratike të shoqërisë, për shembull përmes fushatave të keqinformimit dhe ndikimit. Keqinformimi mund të përdoret për të shpërndarë qëllimisht informata të rreme ose mashtruese me qëllim të ndikimit në qëndrimet, pikëpamjet dhe veprimet e personave në një drejtim të caktuar. Fushatat e ndikimit kontrollohen nga qendra, dhe ngërthejnë edhe përdorimin e një spektri të gjerë të metodave, të hapura dhe të fshehta, një nëngrup i të cilave mund të jetë ndërhyrja në të dhëna dhe sulme të tjera kibernetike. Ato gjithashtu mund të përfshijnë instrumente të fuqisë politike, diplomatike, ekonomike dhe ushtarake. Përhapja e informatës së pasaktë ose çorientuese rrezikon të dëmtojë besimin në institucionet tona publike dhe të sfidojë sigurinë e shoqërisë. Trajtimi kritik i burimeve të informacionit dhe qasja në një shumëllojshmëri të mediave të dhe agjencive të lajmeve të pavarura fuqizjonë vetëdijësimin dhe neutralizojnë efektet e fushatave të keqinformimit dhe ndikimit.

7.1.5. Modeli kombëtar për angazhimet sistematike në sigurinë kibernetike

Siç u përshkrua më lartë, shoqëria e informacionit, qeverisja elektronike dhe ekonomia digjitale po përjetojnë një ritëm të shpejtë të zhvillimit. Njëkohësisht, hapësira kibernetike po përballet me kërcënime të reja. Më shumë se kurrë, shihet domosdoshmëria e njësistemi kombëtar të strukturuar të sigurisë kibernetike që duhet të zhvillohet dhe avancohet në mënyrë që të jetë në gjendje të përballojë sfidat e reja të cilat po paraqiten. Në vijim është paraqitur struktura qeverisëse e cila duhet të udhëheqë punën në fushën e sigurisë kibernetike në Kosovë. Prandaj, zhvillimi i sigurisë kibernetike në nivel kombëtar është objektivë kyçe e strategjisë, dhe kërkon zhvillimin e mëtejmë të strukturave që merren me sigurinë kibernetike në nivel strategjik dhe veprues.

Për të bërë të mundur këto zhvillime, Qeveria e Kosovës do të përgatis dhe implementoj legjislacionin e ri për sigurinë kibernetike ku do të përcaktohen kompetencat e rishikuara të institucioneve përkatëse. Bazuar në ligjin përkatës, Agjencia e Sigurisë Kibernetike do të krijohet si një agjenci ekzekutive, që do të rregullojë përgjesgjësitë e dy kategorive kryesore të entiteve: Operatorëve të Shërbimeve Esenciale dhe Ofruesve të Shërbimeve Digjitale. Në kategorinë e OSHE bëjnë pjesë subjektet publike ose private të cilat posedojnë IKK bazuar në Ligjin për Infrastrukturën Kritike[5]. Me aprovimin e këtij legjislacioni, struktura e propozuar qeverisëse e sigurisë kibernetike në Kosovë do të duket si në vijim:

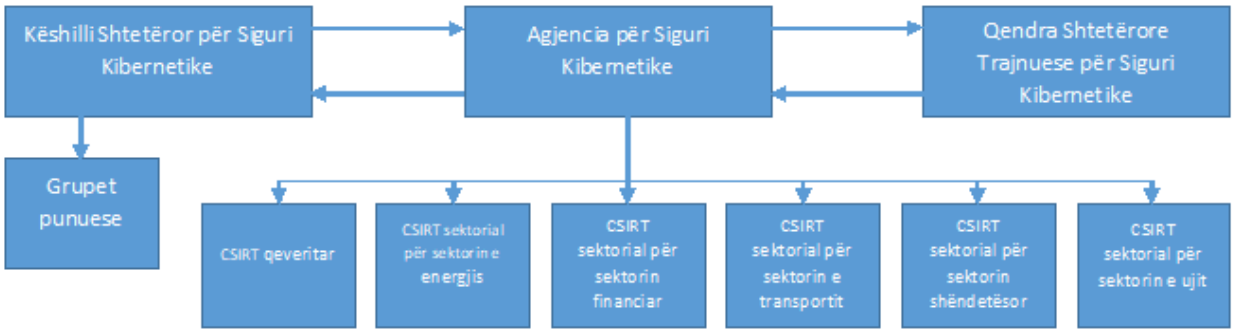

Figura 1. Struktura qeverisëse e sigurisë kibernetike në Kosovë

7.1.6. Harmonizimi institucional

Aktualisht, aktivitetet dhe përgjegjësitë institucionale në fushën e sigurisë kibernetike janë të fragmentuara dhe shpërndara ndërmjet entiteve të ndryshme të sektorit publik dhe privat, gjë që rezulton në efikasitet të kufizuar në këtë fushë. Për të përmirësuar këtë situatë, është e nevojshme të ketë një konsolidim dhe harmonizim të detyrave dhe përgjegjësive të institucioneve të ndryshme përgjegjëse për sigurinë kibernetike. Institucionet, gjegjësisht, palët e interesit të përfshira në sigurinë kibernetike, duhet të punojnë ngushtë me njëra-tjetrën për të identifikuar rolet dhe përgjegjësitë e tyre, si dhe burimet që i kanë në dispozicion, dhe për të ofruar informata hyrëse të hapura dhe transparente për KShSK dhe ASK.

Është e nevojshme të krijohen zgjidhjet sisteme për shkëmbimin e informacionit ndërmjet palëve të interesit dhe shkëmbimin e njohurive për teknologjitë e cenueshme ose joefektive, kërcënimet dhe incidentet e sigurisë kibernetike. Për t'u siguruar që i tërë ekosistemi do të funksionojë në mënyrë efektive, duhet të sqarohet edhe relacioni ndërmjet të gjitha palëve të interesit në sistemin kombëtar të sigurisë kibernetike, duke përfshirë organet përgjegjëse për sigurinë kombëtare, kundër terrorizmin, sigurinë e brendshme dhe rendin publik, prokurorinë publike dhe gjyqësinë.

[5] https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313

Mbivendosja në përgjegjësitë ligjore duhet të reduktohet, ndërsa kontradiktat duhet të identifikohen dhe mënjanohen.

Koordinatori kombëtar për siguri kibernetike (KKSK) do të jetë personi i cili kryeson KShSK.

KKSK-ja në përputhje më legjislacionin në fuqi koordinon aktivitetet me vendimmarrësit përkatës teknik ose ekzekutiv të të gjithë akterëve. Këta vendimmarrës nga ana e tyre do të duhet të komunikojnë në nivel punues me furnitorët, partnerët e rrjetet e tyre, ose edhe të ndërtojnë format e bashkëpunimit brenda të cilave do të diskutojnë, evoluojnë dhe zbatojnë iniciativat strategjike.

Përgjegjësitëdhe koordinimi në sistemin kombëtar të sigurisë kibernetike do të përcaktohen më saktë me akte nënligjore. Kjo do të përfshijë detyrimet dhe kompetencat e mekanizmave dhe subjekteve të sistemit, si dhe mënyrat në të cilat KKSK mund të punojë me palët e interesit të sistemit. KKSK dhe KShSK duhet të kujdesen për të shmangur mbivendosjet, ndërtuar dhe shpërndarë resurset, zbatuar bashkëpunimin ndërqeveritar dhe partneritetin publiko privat, dhe për të identifikuar dhe mënjanuar në mënyrë rigoroze aktivitetet dhe personelin jofunksional.

Grupi Punues për Sigurinë Kibernetike në Infrastrukturën Kritike (GPSKIK) do të jetë një grup këshillues me shumë palë të interesit, që do të inkorporohet në strukturën e KShSK. *Qëllimi i grupit punues është që të ofrojë mbështetje të përgjithshme për rritjen e* qëndrueshmërisë së sigurisë kibernetike të IKK-së. Grupi do të përbëhet nga përfaqësues nga agjencitë dhe ministritë përkatëse qeveritare, sektori privat dhe akademia. Kjo do të sigurojë që të gjithë akterët përkatës të kontribojnë në hartim të politikave, krijojë mundësi për dialog ndërmjet sektorit publikdhe privat, dhe do të mundësojë sigurimin e mbështetjes nga palët e interesit për implementimin e politikave të reja në fushën e sigurisë kibernetike.
Grupi Punues për Sigurinë Kibernetike në Infrastrukturën Kritike ka për synim që të:

i. Ndërtojë kapacitete institucionale për të avancuar qëndrueshmërinë e sigurisë kibernetike të IKK-së ;
ii. Krijojë një platformë kombëtare për shkëmbimin e informacionit për sigurinë kibernetike, dhe
iii. Të shtyjë përpara zhvillimin e institucioneve të sigurisë kibernetike në Republikën e Kosovës.

7.1.7. Sistemi i menaxhimit të rrezikut në nivel kombëtar

Korniza e Sigurisë Kibernetike NIST[6], përfshin menaxhimin e rrezikut si një nga parimet e tij thelbësore dhe pret që adoptuesit e kornizës të praktikojnë menaxhimin e rrezikut dhe të ndërmarrin aktivitete përkatëse. Megjithatë, çdo shtet e vendosë se si të praktikojë menaxhimin e rrezikut që parashihet në kuadër të kësaj kornize. Me qëllim të avancimit të sigurisë kibernetike dhe asaj kombëtare, ASK duhet të adoptojë një sistem kombëtar koherent për vlerësim të rrezikut

[6] https://www.nist.gov/

kibernetik. Ky sistem i vlerësimit të rrezikut duhet të marrë në konsideratë specifikën e sektorëve dhe operatorëve të IKK-ve, si dhe ofruesve të shërbimeve digjitale. ASK do të bëj monitorimin teknik dhe taktik të aftësive të akterëve të ndryshëm që përballën me kërcënimet relevante kibernetike.

Kjo përfshin gjithashtu koordinimin e njohurive në lidhje me cenueshmëritë dhe kërcënimet në kuadër të sistemit kombëtar për vlerësim të rrezikut kibernetik. Vlerësimet e rrezikut mund të mbështeten edhe nga stafi akademik i kualifikuar.

Po ashtu, Qeveria e Kosovës ka për synim edhe themelimin e **Ekipit Kombëtar për Reagime të Shpejta** (**EKRSH**)[7] si një njësi e cila do të ofrojë ndihmë teknike konkrete në veprimet e nevojshme për adresimin e kërcënimeve ose cenueshmërive.

EKRSH do të ketë rol të monitorimit të rregullt, që përfshinë kontrollimet periodike për cenueshmëritë si dhe përditësimet adekuate (patch-at) duke mbajtur një kontakt të shpeshtë me departamentet e sigurisë të prodhuesve të pajisjeve dhe sistemeve të informacionit. EKRSh do të hartoj udhëzues të zbatimit për çdo patch dhe zgjidhje anashkaluese, kurdo që shihet e nevojshme, po ashtu edhe të prodhojë video udhëzime brenda 24 orëve nga publikimi i një patch-it apo zgjidhjeje anashkaluese të re. Duhet të krijohet një model i sigurt komunikimi me të gjitha palët e përfshira. EKRSh duhet të komunikoj shpesh me prodhuesit dhe operatorët dhe të ndërtojë besim dhe bashkëpunim me ta. EKRSh gjithashtu mund t'u ofrohet vendeve fqinje mike si një mjet diplomatik për mësim dhe mbështetje, dhe si një MNSB. Nga ana e tyre, shtetet mike me gjasë do të vlerësojnë një ndihmë të tillë të ofruar, dhe do të jenë më të hapura për forma të tjera të bashkëpunimit, që do të mundësojë rritjen e rrjetit të bashkëpunimit.

EKRSh do të strukturohet në kuadër të ASK dhe do të ndihmoj në përgatitjen e vlerësimit kombëtar të kërcënimeve dhe rrezikut bazuar në një metodologji të vendosur të vlerësimit të rrezikut. ASK do të monitorojë dhe realizojë ri-vlerësime në baza të rregullta rezultatet e të cilave duhet t'i publikojë edhe në raportin vjetor.

Pasi të arrihet një pjekuri në funksionimin e saj, ASK do punojë në zhvillimin e një cyber range[8], për të provuar dhe zbatuar teknologji të reja dhe për t'i përdorur ato në iniciativa të ndryshme teknologjike. Gjetjet duhet të mbahen të përditësuara dhe duhet të ndahen me prodhuesit e TI-së mbi baza të besimit të ndërsjellë.

Kur nuk është në përdorim nga ASK dhe institucionet qeveritare, cyber range mund t'u jepet me qira *startupeve* të sigurisë kibernetike të Kosovës për të promovuar zhvillimin e tyre, për të trajnuar ekipet e kuqe (read teams) që luajnë rolin e një armiku ose kundershtari, dhe për të bërë testime interne të pjekurisë së produkteve të tyre.

[7] Ekipet e Reagimit të Shpejtë kryesisht të njohura brenda kompanive, por mund të zgjerohen në nivelin shtetëror në vendet më të vogla. Ato përbëhen nga administratorë të sistemit me njohuri të mjaftueshme për patch-im në vertikale specifike dhe profesionistët e tillë mund të sigurohen dhe angazhohen më lehtë se sa pozitat e rëëdomta në fushën e sigurisë kibernetike. Ata duhet të punojnë në një gamë prioritetesh, CNI, Mbrojtje, Qeveri, Privat.

[8] https://www.cyberwiser.eu/content/what-cyber-range

Një nga mekanizmat që duhet të implementohen është edhe krijimi i një sistemi të shpërblimit për raportim të cenueshmërive. Ndërtimi i besimit mbetet parakushti kryesor për të pasur raportim dhe shkëmbim mirëfillt të informacionit.

Gjashtë objektivat specifike të cilat do të ndihmojnë në zbatimin e objektivit të përgjithshëm strategjik 1 janë siç vijon:

- ***Objektivi specifik 1****:* Zhvillimi i kornizës ligjore për siguri kibernetike dhe mbrojtje të IKK-së në përputhje me acquis të BE-së. Kjo kornizë duhet të përputhet me direktivat dhe rregulloret që burojnë nga BE.
- ***Objektivi specifik 2:*** Krijimi i një katalogu të IKK-së, vlerësimi i maturitetit aktual për sigurinë kibernetike dhe hartimi i një plani shumëvjeçar për të arritur nivelin e nevojshëm të mbrojtjes.
- ***Objektivi specifik 3:*** Ndërtimi i autoriteteteve kombëtare qendrore për sigurinë kibernetike me mandatin për të zbatuar ligjet, për të zhvilluar dhe mbikëqyrur zbatimin e strategjisë kombëtare dhe për të harmonizuar përpjekjet në nivelin më të lartë.
- ***Objektivi specifik 4:*** Fuqizimi i CERT kombëtar dhe kapaciteteve tjera reaguese ndaj incidenteve kibernetike duke ndërtuar një fuqi punëtore efektive më të madhe dhe pajisur atë me përgjegjësi dhe aftësi ekzekutive në lidhje me sigurinë kibernetike të IKK-së. Kjo përfshin një funksion auditues për auditimin dhe publikimin e efektivitetit të teknologjive të sigurisë kibernetike dhe një funksion të shkëmbimit të informacionit ndërmjet entiteteve qeveritare.
- ***Objektivi specifik 5:*** Nxjerrja e standardeve teknike efektive për nivele të ndryshme të sigurisë, publikimi i udhëzimeve[9] dhe krijimi i një funksioni mbështetës për zbatimin dhe mirëmbajtjen e standardeve.
- ***Objektivi specifik* 6:** Zhvillimi i një qasjeje strategjike kombëtare për prokurimin dhe funksionimin e teknologjive të informacionit më pak të cenueshme në qeveri dhe sektorët kritik privat. Kjo përfshin një kornizë ligjore për kopje rezervë[10] të rregullt dhe përditëso, (patch-im) të shpejtë.

7.2. Objektivi Strategjik 2: Promovimi i programeve vetëdijesuese për sigurinë kibernetike dhe i një kulture të sigurisë kibernetike në Kosovë

Një vlerësim më i mirë i kërcënimeve me të cilat përballet hapësira kibernetike është hap vendimtar për të qenë në gjendje t'i luftojmë ato. Përderisa Qeveria e Kosovës e pranon rolin e saj në krijimin e një mjedisi më të sigurt për gjithë qytetarët e saj, qeveria së bashku me sektorin privat dhe komunitetin kanë një rol të rëndësishëm të përbashkët në zbatimin e kësaj strategjie. Pra, zbatimi

[9] https://www.ncsc.gov.uk/section/advice-guidance/all-topics

[10] Cenueshmëritë e publikuara shpejt shfrytëzohen si mjete sulmi që përdoren kundër objektivave nga shumica e hakerëve. Nëse koha e korrigjimit është më e vogël ose e barabartë me kohën e nevojshme për shfrytëzimin e cenueshmërisë, këtyre hakerëve iu mohohet mundësia të sulmojnë. Mbetet mundësia e sulmit vetëm nga hakerët që përdorin cenueshmëritë zero-ditëshe, të cilët janë shumë më të rrallë dhe kryesisht sulmojnë vetëm caqe me vlerë të lartë. Prandaj, patching-u (arnimi) i softuerëve shpejt zvogëlonshumë rreziqe.

i suksesshëm i kësaj strategjie mbështetet në përpjekjet dhe veprimet individuale dhe bashkëpunuese nga të gjithë akterët përkatës. Qeveria e Kosovës ka synim të ndërtojë një sistem efektiv dhe gjithëpërfshirës të partneritetit publik-privat të bazuar në besimin e ndërsjellë dhe përgjegjësinë e përbashkët për sigurinë tonë kombëtare në hapësirën kibernetike. Duhet të ndërmerren hapa kolektiv për të mbrojtur Kosovën nga sulmet e mundshme, propaganda armiqësore apo çfarëdo forme tjetër ç'rregulluese.

Në mbështetje të këtij objektivi, qeveria do të krijojë një sistem të kërkimit dhe zhvillimit për projekte që e përfshijnë dhe tejkalojnë fushën e sigurisë kibernetike tradicionale, për të kuptuar kërcënimet ekzistuese dhe ato të potenciale, duke përfshirë përndjekjen kibernetike (cyberstalking), gjuhën e urrejtjes dhe keqinformimin. Kompetenca dhe njohuritë rreth kërcënimeve, cenueshmërive dhe masave efektive, përbëjnë një parakusht për mbrojtjen e IKI-së. Me zhvillimin e IoT, qyteteve inteligjente, Industrisë 4.0, Cloud Computing dhe Big Data, shtohet nevoja për t'i ngritur aktivitetet e kërkimit, dhe zhvillimit në sigurinë kibernetike.

Sa i përket shkathtësive dhe fushave të interesit, kërkimi që synon krijimin e aftësive kombëtare për kriptim dhe zhvillimin e një algoritmi kombëtar të kriptimit për nevoja kombëtare, mund të rezultojë i dobishëm. Përndryshe, duhet punuar me algoritme të mirënjohura të kriptimit si p.sh. *RSA*[11] ose të ngjashme.

Përveç kësaj, do të zhvillohen kurse bazike të sigurisë kibernetike. Këto kurse do të përfshijnë një planprogram që mëson bazat e hakerimit, në nivel universitar, por çka është më e rëndësishmja, një version i tij do të zhvillohet për nxënësit e shkollave të mesme, duke u siguruar që të jetë një kurs gjithëpërfshirës, tërheqës dhe të përfshijë vajza të reja të cilat do të përfitonin shumë nga njohuritë e tilla, gjë që do të ndihmonte edhe në adresimin e hendekut gjinor.

Ekziston një hendek i qartë i aftësive të sigurisë kibernetike të raportuara në administratën publike të Kosovës, sa i përket mungesës të burimeve njerëzore të kualifikuara për të punuar në këtë fushë. E edhe më i spikatur është hendeku i dukshëm gjinor në këtë fushë.

Specialistët e sigurisë kibernetike duhet t'i mbulojë nevojat e tregut të punës dhe kërkesat e sigurisë kombëtare. Inkuadrimi i më shumë grave dhe vajzave në sigurinë kibernetike do t'i jepte shtytje industrisë dhe do të plotësonte nevojën drastike që të gjithë sektorët dhe palët e interesit kanë për talentë të nivelit të lartë.

Duhet të hartohet një plan gjithëpërfshirës afatgjatë për të krijuar shkathtësitë kombëtare në këtë fushë , duke i përfshirë masat për të ngritur vetëdijen e publikut të gjerë. Higjiena kibernetike [12], shkathtësitë digjitale, vetëdijësimi mbi kërcënimet moderne kibernetike dhe përballja me ato duhet të bëhen pjesë integrale e edukimit të secilit qytetar të Kosovës.

[11]RSA: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[12] Higjiena kibernetike është një grup praktikash që organizatat dhe individët kryejnë rregullisht për të ruajtur shëndetin dhe sigurinë e përdoruesve, pajisjeve, rrjeteve dhe të dhënave. Qëllimi i higjienës kibernetike është të mbajë të sigurta të dhënat e ndjeshme dhe t'i mbrojë ato nga vjedhjet ose sulmet

Objektivi strategjik 2 do të zbatohet me ndihmën e katër objektivave specifike si më poshtë:

- ***Objektivi specifik* 1**: Zhvillimi dhe zbatimi i fushatave vetëdijësuese që do të mbulojnë sektorë të ndryshëm brenda qeverisë dhe institucioneve tjera publike, IKK-të, sektorin privat dhe shoqërinë civile;
- ***Objektivi specifik* 2**; Krijimi i fushatave, konferencave dhe programeve civile dhe akademike, duke i përfshirë të gjitha pjesët e shoqërisë në nxitjen e një dialogu të vazhdueshëm për sigurinë kibernetike;
- ***Objektivi specifik* 3:** Promovimi i kërkimt, zhvillimit, mësimdhënies,trajnimit në siguri kibernetike dhe mbrojtje të të dhënave në universitet;
- ***Objektivi specifik* 4:** Krijimi i një programi arsimor STEM në shkolla, duke përfshirë komponentë të sigurisë kibernetike për të frymëzuar më shumë vajza që të zgjedhin karrierën e punës në siguri kibernetike. Kjo duhet të konsiderohet si një prioritet i lartë pasi lehtësisht dyfishon fuqinë punëtore ekzistuese.

7.3. Objektivi Strategjik 3: Mbështetja e zhvillimit të sektorit privat në sigurinë kibernetike, PPP-së dhe shkëmbimit te informacionit ndër sektorial

Garantimi i sigurisë dhe qëndrueshmërisë të domenit dhe infrastrukturës digjitale të Kosovës është një përgjegjësi e përbashkët ndërmjet disa palëve të interesit. Kjo është veçanërisht e vërtetë duke pasur parasysh se as qeveria e as sektori privat vetëm për vetëm nuk kanë njohuri, autoritet apo burime për të bartur ekskluzivisht këtë përgjegjësi.

Partneritetet publiko-private janë themeli i zbatimit efektiv të strategjisë së sigurisë, si dhe shkëmbimi në kohë dhe i besueshëm i informacionit ndërmjet palëve të interesit është thelbësor për sigurinë e Kosovës.[13]

Krijimi i një kuadri të PPP-së do të mundësojë shkëmbimin e njohurive, e praktikave më të mira dhe nivelin e përbashkët të mirëkuptimit ndërmjet të të gjithë akterëve. Sipas ENISA[14] motivimi kryesor nga sektori publik dhe privat për t'iu bashkuar PPP-së është ngritja e nivelit të sigurisë kibernetike. Rritja e bashkëpunimit do të çojë në: vetëdijësim më të mirë për situatën, vendimmarrje më të mirë, rritje të besimit, qasje më të mirë në burime, si dhe një kuptim më të mirë të mbrojtjes të IKI dhe sigurisë kibernetike në përgjithësi.[15]

Marrëveshjet PPP përmirësojnë komunikimin, planifikimin, vlerësimin e rrezikut, zbatimin e programit dhe aktivitetet operacionale, duke përfshirë edhe reagimin ndaj incidenteve dhe rikuperimin nga to.

[13] Agjencia e Bashkimit Evropian për Sigurinë e Rrjetit dhe Informacionit (ENISA): Modelet e Bashkëpunimit të Partneriteteve Publike Private (PPP), nëntor 2017.
[14] Ibid.
[15] Agjencia e Bashkimit Evropian për Sigurinë e Rrjetit dhe Informacionit (ENISA): Modelet e Bashkëpunimit të Partneriteteve Publike Private (PPP), faqe *13*, nëntor 2017.

Partneritetet e tilla do të ndihmojnë në zbatimin e aktiviteteve të sigurisë dhe qëndrueshmërisë në tërë Kosovën dhe do të përfshihen në sistemin kombëtar të sigurisë kibernetike.

Është e rëndësishme se Qeveria e Kosovës do të zhvillojë një sistem për të promovuar themelimin e *startup*-eve të sigurisë kibernetike në Kosovë. Talenti për inovacion në Kosovë është evident, dhe *startup*-ët ofrojnë një strukturë të mirë nxitëse për talentët e rinj për t'i lidhur ata me kauzën e sigurisë kibernetike në nivel kombëtar. Startup-ët e sigurisë kibernetike mund të financohen me investimet ndërkombëtare, natyrisht nëse ofrohen kushte tërheqëse si taksat e ulëta dhe kontratat qeveritare për produkte funksionale. Ato mund të ndihmojnë në krijimin e një fuqie të madhe punëtore të specializuar për të mbështetur punën e përgjithshme të sigurisë kibernetike dhe për të sjellë përfitime ekonomike për Kosovën. Thelbësore për krijimin e një kulture të tillë të *startup-ëve* është krijimi i një bërthame efektive të njohurive dhe trajnimeve të motivuara nga ndërmarrësia dhe të informuara nga industria, të cilat mund të zhvillohen në universitetet e aplikuara ose në ushtri, ku tashmë është duke u punuar në krijimin e një qendër trajnuese për sigurinë kibernetike.

Objektivi strategjik 3 do të zbatohet me ndihmën e dy objektivave specifike në vijim:

- ***Objektivi specifik* 1:** Krijimi i grupeve punuese të Partneritetit Publik Privat dhe nxitja për themelimin e grupeve punuese të veçanta brenda sektorit privat, për shkëmbimin e informacionit mbi kërcënimet dhe produktet e sigurisë kibernetike
- ***Objektivi specifik* 2:** Zhvillimi i stimujve dhe i një bërthame për *startup-ët* e sigurisë kibernetike në Kosovë, si dhe ftimi i investimeve të huaja strategjike dhe financiare përmes mekanizmave të veçantë dhe tërheqës për investime.
  Kjo duhet të konsiderohet si një prioritet i lartë pasi mund të zgjidhë shumë çështje në mënyrë të qëndrueshme, duke u financuar nga jashtë dhe duke gjeneruar përfitime ekonomike për Kosovën në planin afatgjatë.

7.4. Objektivi Strategjik 4: Ndërtimi i bashkëpunimit të qëndrueshëm dhe të dobishëm kombëtar dhe ndërkombëtar në sigurinë kibernetike

A. Bashkëpunimi ndërkombëtar në nivel strategjik dhe politik

Me qëllim të promovimit të një hapësire të sigurt dhe të besueshme ndërkombëtare kibernetike, dhe në mbështetje të interesave kombëtare, Qeveria e Kosovës do të angazhohet edhe ndërkombëtarisht në:

a. Rritjen e pranisë të Kosovës në organizatat dhe forumet ndërkombëtare dhe rajonale për sigurinë kibernetike.
b. Promovimin e bashkëpunimit ndërkombëtar në sektorët legjislativ, gjyqësor dhe policor në luftën kundër krimit dhe spiunazhit kibernetik;
c. Përmirësimin e protokollit dhe procedurave për komunikim diplomatik me qëllim që Kosova të bëhet një partner ndërkombëtar i besueshëm dhe kredibil në luftimin e

kërcënimeve kibernetike dhe në qëndrimin e unifikuar për të mbrojtur të drejtat e njeriut në këtë hapësirë.

d. Nxitjen e bashkëpunimit me NATO-n në mbrojtjen kibernetike, veçanërisht në lidhje me reagimin ndaj incidenteve kibernetike dhe shkëmbimin e informacionit teknik mbi kërcënimet dhe cenueshmëritë;
e. Në bashkëpunimin dhe harmonizimin e legjislacionit kombëtar me BE, duke promovuar një politikë ndërkombëtare në hapësirën kibernetike.

B. **Bashkëpunimi ndërkombëtar në nivel teknik dhe veprues**

Bashkëpunimi ndërkombëtar me BE-në, NATO-n dhe shtetet të tjera mike duhet të fuqizohet. Duhet të synohet gjendja ku kryerja e sulmeve kibernetike ndaj Kosovës do të jetë e vështirë dhe me pasoja për sulmuesit. Kosova duhet të kontribuojë në mënyrë aktive në sigurimin e një hapësire të hapur, të sigurt dhe të besueshme të internetit, si edhe në mbrojtjen e infrastrukturës kritike të TIK dhe IKI-së.

Përveç kësaj, Kosova gjithashtu duhet të marrë pjesë në dialogun teknik ndërkombëtar dhe të zhvillojë rrjetin e saj ndërkombëtar duke mësuar nga përvoja e institucioneve dhe partnerëve ndërkombëtarë që veprojnë me sukses në sigurinë kibernetike.

Institucionet e Kosovës do të bëjnë përpjekje për t'i identifikuar dhe për t'iu bashkuar ushtrimeve teknike dhe trajnimeve te standardizuara ndërkombëtare. Kosova do të fuqizojë bashkëpunimin ndërkombëtar në sigurinë kibernetike duke mbështetur iniciativat ndërkombëtare të cilat i përmbushin interesat kombëtare të Kosovës dhe zgjerojnë dialogun e Kosovës me BE-në, NATO-n dhe OSBE-në. Për të fuqizuar mbrojtjen dhe diplomacinë e sigurisë kibernetike, Kosova do të ndërmarrë veprimet si më poshtë:

a. Vendosja e bashkëpunimit me ICANN për të zhvilluar politika publike në Internet;
b. Shqyrtimi i mundësive për anëtarësimin e Kosovës në Strategjinë e BE-së për të zbatuar DNS dhe për të diversifikuar njohjen e emrit DNS, si dhe për të mbështetur iniciativën DNS për BE për të shmangur skenarët ekstremë të sulmeve kibernetike në shtegun global të DNS;
c. Kërkimin e mundësive për miratimin dhe zbatimin e rregullores së BE-së për IPv6, jo vetëm për shkaqe ekonomike, por edhe për qëllime të zbatimit të ligjit;
d. Fuqizimi i bashkëpunimit më ENISA, specifikisht, por pa u kufizuar vetëm në, reagimin ndaj incidenteve, zbulimin e kërcënimeve dhe zhvillimin e fuqisë punëtore;
e. Krijimi i një bashkëpunimi me ITU në standardizimin e sigurisë kibernetike dhe komunikimeve elektronike;
f. Rritja e bashkëpunimit bilateral dhe multilateral me CERT-ët kombëtar të shteteve tjera

Objektivi strategjik 4 do të zbatohet me ndihmën e tri objektivave specifike si më poshtë:

- ***Objektivi specifik* 1:** Nxitja e bashkëpunimit kombëtar në të gjithë sektorët dhe hapja e Kosovës si një akter kompetent për bashkëpunim ndërkombëtar në nivel rajonal dhe global

- ***Objektivi specifik* 2:** Pjesëmarrja në përpjekjet diplomatike rreth normave kibernetike
- ***Objektivi speifik* 3:** Bashkëngjitja në konventat për sigurinë dhe krimin kibernetik dhe marrëveshje të tjera relevante ndërkombëtare
- ***Objektivi Strategjik* 4:** Ofrimi i Kosovës si terren për ushtrime kibernetike ushtarake dhe pjesëmarrja në ushtrime kibernetike.

7.5. Objektivi Strategjik 5: Zhvillimi i kapaciteteve të qëndrueshme të sigurisë kibernetike për qeverinë dhe sektorin privat

Zhvillimi i kapaciteteve të qëndrueshme paraqet mbase sfidën më të madhe në sigurinë kibernetike. Një numër i madh vendesh dhe shumë kompani po dështojnë në këtë aspekt, dhe kjo ka një ndikim të madh në pozicionin e përgjithshëm strategjik dhe posturën e sigurisë. Zhvillimi i burimeve njerëzore dhe stafit kompetent kërkon një kohë të gjatë, së paku disa vite. Përveç kësaj, fuqia punëtore e TIK-ut mund të jetë mjaft e paqëndrueshme për sa i përket ndërrimit të punëdhënësve, dhe kjo është veçanërisht e vërtetë në rastin e profesionistëve të TIK-ut në shërbimin publik, dhe kalimi i punëtorëve kompetentë në sektorin privat. Madje edhe brenda sektorit privat ka shumë konkurrencë dhe lëvizje të punëtorëve.

Ndërtimi dhe mbajtja e stafit kompetent është prioritet kyç për Kosovën. Natyra dinamike e sfidave të sigurisë kibernetike kërkon zhvillimin e vazhdueshëm të kapaciteteve dhe aftësive të nevojshme. Për këtë, Qeveria e Kosovës do të promovojë:

g. Zhvillimin e planit të ndërtimit të kapaciteteve për të adresuar kërkesat specifike të Kosovës për aftësitë që nevojiten për të përmbushur sfidat gjithnjë në rritje të adresimit të kërcënimeve të sigurisë kibernetike, dhe
h. Zhvillimin e strategjive të rekrutimit dhe mbajtjes që synojnë të sigurojnë zhvillimin dhe mirëmbajtjen e një niveli të mjaftueshëm të ekspertizës.

Objektivi strategjik 5 do të zbatohet me ndihmën e tri objektivave specifike si më poshtë:

- ***Objektivi specifik* 1:** Hapja e funksioneve kyçe të qeverisë për mbështetje nga sektori privat ose kontraktimin e pjesshëm të jashtëm për t'i përmbushur boshllëqet kritike të njohurive. Kjo është një masë që mund të shihet si e pazakontë, por që është e rëndësishme për të mbushur ato boshllëqe.
- ***Objektivi specifik* 2**; Zhvillimi i një programi kombëtar trajnimi dhe edukimi për sigurinë kibernetike në sektorin akademik në bashkëpunim me subjekte të specializuara të sektorit privat;
- ***Objektivi specifik* 3:** Reformimi i mekanizmave të pagave publike dhe të prokurimit për të hapur Kosovën ndaj ekspertëve të kushtueshëm brenda qeverisë dhe për prokurim të shpejtë të teknologjive kritike.

7.6. Objektivi Strategjik 6: Avancimi i aftësive hetimore dhe ushtarake të sigurisë kibernetike

Natyra pa kufij e krimit kibernetik, ka kontribuar në përhapjen e gjerë të aktiviteteve kriminale ku përfshihen kompjuterët dhe sistemet e informacionit, qoftë si mjet apo cak parësor. Kërcënimet kibernetike vijnë si nga akterët jo-shtetërorë ashtu edhe nga ata shtetërorë. Ato janë shpesh të natyrës kriminale, të motivuara nga fitimi, por mund të jenë edhe me motive politike dhe strategjike. Prandaj, siguria kibernetike po bëhet gjithnjë e më shumë një çështje kritike për sigurinë kombëtare. Si i tillë, krimi kibernetik nuk ka ndikim vetëm në ekonomi, por edhe në funksionimin e demokracive, lirive sociale dhe vlerave humane.

Mjegullia e kufirit ndërmjet krimit kibernetikë dhe krimit "tradicional" intensifikon kërcënimin kriminal, pasi kriminelët përdorin internetin si një mënyrë për të rritur aktivitetet e tyre, por edhe si një burim për të gjetur metoda dhe mjete të reja për të kryer krimin. Megjithatë, në shumicën dërrmuese të rasteve, gjasat për të gjurmuar kriminelin janë minimale dhe gjasat për ndjekje penale janë akoma më të vogla.

Qeveria e Kosovës ka ndërmarrë hapat e nevojshëm në ngritjen e infrastrukturës ligjore që synon parandalimin dhe luftimin e të gjitha formave të krimit kibernetikë. Njësia për Hetimin e Krimeve Kibernetike në kuadër të Policisë së Kosovës, posedon kapacitete teknike dhe trajnime të nevojshme për t'i hetuar krimet kompjuterike.

Megjithatë mbeten shumë sfida, veçanërisht sfidat teknike të cilat i pengojnë autoritetet të merren me sukses me këtë formë të kriminalitetit. Ndërkohë që janë ndërmarrë hapat fillestarë, mbetet për t'u vendosur një përgjigje më efektive e zbatimit të ligjit duke u fokusuar në zbulimin, gjurmimin dhe ndjekjen penale të kriminelëve kibernetik. Është thelbësore që të ndërtohet besimi tek qytetarët se të gjitha llojet e krimit trajtohen me përgjegjësi dhe efektivitet.

Në vitet e fundit në Kosovë vërehet një rritje e konsiderueshme e përdoruesve të internetit , gjë që ka sjellë me vete një rrezik të shtuar sa i përket krimeve dhe sulmeve kibernetike. Edhe pse deri më tani nuk ka pasur raste të depërtimit dhe dëmtimit serioz të sistemeve me të dhëna shtetërore, aktivitetet e ndryshme kriminale kanë mjaftuar për të evidentuar dobësitë e rrjeteve kompjuterike në Kosovë. Sipas të dhënave në dispozicion, objektivat kryesore të sulmeve kompjuterike në Kosovë deri më tani janë llogaritë e përdoruesve, sistemet bankare dhe faqet e internetit. Qeveria e Kosovës do të përmirësojë kushtet që policia të kryejë detyrat e saj në përputhje me zhvillimet teknologjike dhe trendet e krimit.

Shumë prej mekanizmave të sigurisë pasive nuk i pengojnë sulmuesit. Këta mekanizma thjeshtë rrisin përpjekjen dhe kohën që sulmuesit duhet të shpenzojnë për të kryer sulmin. Mundësitë hetimore mund të rrisin gjithashtu rrezikun për sulmuesit. Prandaj, mundësia bazike për t'i hetuar incidentet kriminale ose spiunazhin është shumë e rëndësishme.

Edhe pse hetimet në disa raste mund të mos japin rezultate të dëshiruara, mospasja e kapaciteteve hetuese nuk mund të shihet si opcion, pasi kjo do ta kthente Kosovën në një cak ose proxy sulmesh, duke gjeneruar shumë probleme kriminale dhe diplomatike për vendin. Posedimi i aftësive të mira

hetimore madje mund të ndihmojë shumë Kosovën për t'u bërë një akter i rëndësishëm ndërkombëtar dhe për të ndërtuar besim dhe lidhje me vendet tjera.

Qeveria e Kosovës synon të ndërtojë mundësi funksionale dhe të fuqishme hetimore. Për t'i fuqizuar aftësitë hetimore, Qeveria e Kosovës ndër të tjera do të:

a. Përmirësojë legjislacionin duke adresuar sfidat dhe tendencat aktuale në fushën e sigurisë kibernetike.
b. Zhvillojë një metodologji për mbledhjen e statistikave kibernetike dhe të publikojë çdo vit informata statistikore mbi sulmet kibernetike.
c. Sigurojë një rritje të nivelit të njohurive të operativëve, punonjësve të organeve të hetimit, prokurorëve, gjyqtarëve në fushën e teknologjisë të informacionit dhe sigurisë kibernetike, dhe më konkretisht në mbledhjen dhe sigurimin e provave digjitale.
d. Lehtësojë angazhimin e ekspertëve të sektorit privat në kërkime në fushën e kompjuterikës dhe telekomunikacionit, në fushën e softuerit dhe fushave të tjera të nevojshme, që do t'i mundësojë ata të përgjigjen shpejt ndaj incidenteve kibernetike dhe të hetojnë në mënyrë efektive krimet kibernetike.

Aktivitetet e planifikuara për realizimin e këtij objektivi strategjik do të klasifikohen dhe nuk do të bëhen publike.

8. INSTITUCIONET PËRGJEGJËSE DHE KORNIZA LIGJORE

8.1. Mekanizmi institucional

Mekanizmi institucional nënkupton të gjithë mekanizmat të cilët kanë rol dhe rëndësi në sigurinë kibernetike në Kosovë.

Mekanizmat institucional për hartimin dhe zbatimin e politikave shtetërore në fushën e sigurisë kibernetike janë por nuk kufizohen në institucionet e mëposhtme:

Zyra e Kryeministrit

Zyra e Kryeministrit është përgjegjëse për përgatitjen e propozimeve të projekt amendamenteve kushtetuese, projektligjeve, projekt akteve nënligjore, koncept dokumenteve (vlerësimit të ndikimit), vlerësimeve Ex-post të legjislacionit, dokumenteve strategjike dhe propozimeve të tjera, nga fushëveprimi i Qeverisë si tërësi dhe i Zyrës së Kryeministrit, si dhe monitorimin dhe sigurimin e zbatimit të tyre. Roli i Zyres së Kryeministrit është mbështetja në realizimin e objektivave strategjike;

Ministria e Punëve të Brendshme (MPB)

MPB është institucioni përgjegjës për hartimin dhe monitorimin e politikave dhe legjislacionit në fushën e sigurisë kibernetike në Republikën e Kosovës. MPB po ashtu ka rolin kryesor në koordinimin e Strategjisë, monitorimin e zbatimit të Planit të Veprimit, si dhe hartimin e raporteve periodike.

MPB është institucioni përgjegjës për zbatimin e ligjit për infrastrukturë kritike dhe identifikimin e IKK-së në Republiken e Kosovës.

Policia e Kosovës si agjenci për zbatimin e ligjit në kuadër të MPB-së, ka përgjegjësinë kryesore në luftimin e të gjitha formave të krimit kibernetik.

Agjencia e Shoqërisë së Informacionit (AShI)

Agjencia e Shoqërisë së Informacionit bën koordinimin, udhëheqjen dhe mbikëqyrjen e proceseve dhe të mekanizmave të qeverisjes elektronike në lidhje me infrastrukturën e TIK-ut, zgjerimin e shërbimeve të internetit në institucionet e Republikës së Kosovës, akumulimin, administrimin, përhapjen dhe ruajtjen e të dhënave, duke krijuar Qendrën shtetërore të të dhënave elektronike si dhe Sigurinë dhe mbrojtjen e infrastrukturës komunikuese elektronike dhe të të dhënave. ASHI sipas nevojës, ndihmon institucionet relevante në luftimin e krimit kibernetik dhe siguron mbrojtjen e të dhënave personale në formë elektronike, në pajtim me legjislacionin në fuqi.

Koordinatori Nacional për Sigurinë Kibernetike

Koordinatori Nacional për Sigurinë Kibernetike është Ministri i Punëve të Brendshme, ose personi i autorizuar nga ai, i cili është përgjegjës të bashkërendojë, udhëzojë, monitorojë dhe të raportojë për zbatimin e politikave, aktiviteteve dhe veprimeve në lidhje me Sigurinë Kibernetike.

Kordinatori Nacional për Siguri Kibernetike udhëheq Këshillin Shtetëror për Siguri Kibernetike.

Sekretariati i Strategjive

Sekretariati i Strategjive ka për funksion grumbullimin e informatave dhe të dhënave nga institucionet e tjera, analizën dhe vlerësimin e informatave të mbledhura, si dhe hartimin e raporteve analitike për Koordinatorin Nacional dhe Këshillin Shtetëror të Sigurisë

Kibernetike. Përveç këtyre, Sekretariati do të shpërndajë me kohë informatat te të gjitha palët përkatëse, duke u bazuar në aktivitetet e planifikuara në Planin e Veprimit për Sigurinë Kibernetike.

Departamenti për Siguri Kibernetike dhe Administrim të Sistemëve
Departamenti për Siguri Kibernetike dhe Administrim të Sistemëve i MPB-së është përgjegjës për përgatitjen e politikave të sigurisë kibernetike dhe mbikëqyrjen e zbatimit të tyre. Ka rol udhëheqës në përgatitjen e strategjisë.

Këshilli Gjyqësor i Kosovës
Siguron që gjykatat në Kosovë të jenë të pavarura, profesionale dhe të paanshme, me qëllim që sistemi gjyqësor të jetë sa më efikas në luftë kundër krimit kibernetik.

Këshilli Prokurorial i Kosovës
Siguron që sistemi prokurorial në Kosovë të jetë i pavarur, i paanshëm dhe profesional në ushtrimin e ndjekjes, hetimit dhe zbulimit të veprave penale të krimit kibernetik dhe të përfaqësojë në gjykata aktet akuzuese në emër të shtetit.

Prokuroritë dhe gjykatat
Janë institucionet përgjegjëse për ndjekjen penale të kryerësve, ndëshkimin adekuat të tyre, për konfiskimin e pasurisë dhe aseteve të fituara me anë të aktiviteteve kriminale.

Sekretariati i Këshillit të Sigurisë së Kosovës
Sekretariati, si pjesë përbërëse e Këshillit të Sigurisë së Kosovës bën përgatitjen e raporteve periodike dhe analizave për Qeverinë e Republikës së Kosovës dhe Këshillin e Sigurisë së Kosovës që kanë të bëjnë me çështjet politike të sigurisë, si dhe ofron ndihmë në hartimin e politikave të sigurisë në Kosovë, përfshirë edhe ndërtimin e kapaciteteve, instrumentet e politikave dhe hulumtimit, ofrimin e mbështetjes administrative dhe funksionale të Këshillit të Sigurisë së Kosovës.

Agjencia e Kosovës për Inteligjencë (AKI)
AKI bën identifikimin e kërcënimeve që rrezikojnë sigurinë e Kosovës. Kërcënim ndaj sigurisë së Kosovës konsiderohet kërcënimi ndaj integritetit territorial, integritetit të institucioneve, rendit kushtetues, stabilitetit dhe zhvillimit ekonomik, si dhe kërcënimet ndaj sigurisë globale në dëm të Kosovës.

Ministria e Drejtësisë (MD)
MD përgatit dhe zhvillon legjislacionin në fushën e drejtësisë, si dhe koordinon dhe zhvillon bashkëpunimin juridik ndërkombëtar në çështjet penale.

Ministria e Mbrojtjes (MM)

Ministria e Mbrojtjes harton politikat e përgjithshme shtetërore të mbrojtjes, kurse Forca e Sigurisë së Kosovës (FSK) zbaton këto politika në mbrojtjen e sovranitetit dhe integritetit territorial, qytetarëve, pronën dhe interesat e Republikës së Kosovës. MM\FSK zhvillon dhe fuqizon mbrojtjen kibernetike për sistemet e MM\FSK-së të bazuara në teknologji të informacionit si dhe ofron mbështetje instiucioneve të Republikës së Kosovës në rast të krizave në vend për mbrojtjen e të dhënave dhe infrastruturës kritike. Përmes Qendrës Shtetërore Trajnuese për Siguri Kibernetike MM\FSK do të ofrojë trajnime në fushën e sigurisë kibernetike për të gjitha institucionet e Republikës së Kosovës.

Ministria e Ekonomisë (ME)
Siguron cilësinë e shërbimeve dhe të standardeve teknike në fushën e telekomunikacionit, krijon politikën e punës për promovimin e konkurrencës në fushën e telekomunikacionit, shqyrton nevojat dhe kërkesat e konsumatorëve në fushën e telekomunikacionit, përkrah teknologjinë e informacionit dhe të inovacioneve, përkrah qasjen në teknologji për të gjithë qytetarët e Kosovës dhe nxit zhvillimin e sistemeve të aftësimit në teknologjinë e informacionit.

Ministria e Financave, Punës dhe Transfereve (MFPT)
MFPT siguron që kostot financiare e aktiviteteve të strategjisë janë brenda kornizave buxhetore. Gjithashtu përmes Doganave, Njësisë së Inteligjencës Financiare dhe Administratës Tatimore, do të ndihmojë në forcimin e sigurisë kibernetike, parandalimin dhe luftimin e krimit kibernetik.

Ministria e Arsimit, Shkencës, Teknologjisë dhe Inovacionit (MAShTI)
MASHTI luan rol të rëndësishëm në fushën e parandalimit dhe vetëdijesimit nëpërmjet hartimit të kurrikulave, organizimit të aktiviteteve vetëdijesuese për përdorimin e internetit dhe aktiviteteve tjera jashtë-programore.

Ministria e Punëve të Jashtme dhe Diaspores (MPJD)
MPJD ka rol në drejtim të dhënies së ndihmës në diplomacinë kibernetike dhe për bashkëpunim ndërkombëtarë në luftën kundër krimit të organizuar.

Autoriteti Rregullativ i Komunikimeve Elektronike dhe Postare (ARKEP)
ARKEP është organi rregullator, i cili zbaton dhe mbikëqyrë kornizën rregullatore të përcaktuar nga Ligji për Komunikime Elektronike, nga Ligji për Shërbimet Postare, si dhe nga politikat e zhvillimit të fushës së komunikimeve elektronike dhe shërbimeve postare.

Agjencia e Kosovës për Forenzikë
Është institucioni përgjegjës për ofrimin e paanshëm, objektivë e professional të ekspertizave shkencore forenzike. Misioni i Agjencisë së Kosovës për Forenzikë është që përmes ushtrimit

të veprimtarisë së saj, të ofroj shërbime forenzike e cilësore në përputhje me legjislacionin në fuqi, standardet vendore dhe ndërkombëtare.

Agjencia për Informim dhe Privatesi (AIP)
AIP siguron që kontrolluesit respektojnë obligimet e tyre rreth mbrojtjes së të dhënave personale dhe se subjektet e të dhënave informohen rreth të drejtave dhe obligimeve të tyre në pajtim me Ligjin për Mbrojtjen e të Dhënave Personale. Gjithashtu ofron këshilla për Kuvendin e Republikës së Kosovës, Qeverinë, organet e pushtetit lokal dhe të gjithë ushtruesit e pushtetit publik në Kosovë lidhur me çështjet për Mbrojtjen e të Dhënave Personale, si dhe këshillon të gjitha institucionet private lidhur me Mbrojtjen e të Dhënave Personale.

8.2. Korniza ligjore

Në fushën e TIK-ut, Republika e Kosovës ka në zbatim një bazë të gjerë ligjore, e cila përfshin por nuk kufizohet në:

- Kushtetuta e Republikës së Kosovës[16];
- Ligji Nr. 06/L-014 për infrastrukturën kritike [17]
- Ligji Nr. 08/L-173 për sigurinë kibernetike [18]
- Ligji nr. 03/L-050 për Themelimin e Këshillit të Sigurisë së Kosovës[19];
- Ligji nr. 04/L-145 për Organet Qeveritare të Shoqërisë së Informacionit[20];
- Ligji nr. 04/L-094 për Shërbimet e Shoqërisë Informatike[21];
- Ligji nr. 04/L-109 për Komunikimet Elektronike[22];
- Ligji nr.05/L-030 për Përgjimin e Komunikimeve Elektronike[23];
- Ligji nr.06/L – 082 për Mbrojtjen e të Dhënave Personale[24];
- Ligji nr. 04/L-076 për Policinë[25];
- Ligji nr. 03/L-142 për Rendin dhe Qetësinë Publike[26];
- Ligji nr. 03/L063 për Agjencinë e Kosovës për Inteligjencë[27];
- Ligji nr. 04/L-149 për Ekzekutimin e Sanksioneve Penale[28];
- Ligji nr. 04/L-065 për të Drejtën e Autorit dhe të Drejtat e Përafërta[29];

[16] http://gzk.rks-gov.net/ActDetail.aspx?ActID=3702
[17] https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313
[18] https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933
[19] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2521
[20] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8669
[21] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2811
[22] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851
[23] https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968
[24] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2676
[25] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2806
[26] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2651
[27] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2538
[28] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8867
[29] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2787

- Ligji nr. 03/ L-183 për Zbatimin e Sanksioneve Ndërkombëtare[30];
- Ligji nr. 04/L-213 për Ndihmën Juridike Ndërkombëtare në Çështje Penale[31];
- Ligji nr. 04/L-052 për Marrëveshjet Ndërkombëtare[32];
- Ligji nr. 04/L-072 për Kontrollin dhe Mbikëqyrjen e Kufirit Shtetëror[33];
- Ligji nr. 04/L-093 për Bankat, Institucionet Mikrofinanciare dhe Institucionet Financiare Jobankare[34];
- Ligji nr. 04/L-064 për Agjencinë e Kosovës për Forenzikë[35];
- Ligji nr. 04/L-198 për Tregtinë e Mallrave Strategjike[36];
- Ligji nr.04/L –004 për Shërbimet Private të Sigurisë[37];
- Ligji nr. 06/L-123 për Forcën e Sigurisë së Kosovës[38];
- Ligji nr. 06/L-122 per Ministrine e Mbrojtjes – *te vendoset referenca*
- Kodi nr. 03/L-109 Doganor dhe i Akcizës i Kosovës[39];
- Ligji nr. 04/L-099 për Ndryshim-Plotësimin e Kodit Doganor dhe të Akcizave në Kosovë, nr. 03/l-109[40];
- Ligji nr.03/L-178 për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë[41];
- Kodi nr. 04/L-082 Penal i Republikës së Kosovës[42;]
- Kodi nr. 04/L-123 i Procedurës Penale[43;]
- Ligji nr.03/L-122 për Shërbim të Jashtëm të Republikës së Kosovës[44];
- Kodi nr.03/L-193 i Drejtësisë për të Mitur[45];
- Rregullore nr.18/2011 për Shpërndarjen dhe Transferimin e Informacionit të Klasifikuar[46].
- Ligj Nr. 06/L-014 për Infrastrukturën Kritike[47]
- Ligji Nr. 08/L-022 për Identifikimin Elektronik dhe Shërbimet e Besuara në Transaksionet Elektronike[48]

Kjo strategji është në përputhje me aktet ndërkombëtare që rregullojnë fushën e sigurisë kibernetike.

[30] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2674
[31] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8871
[32] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2789
[33] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2801
[34] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2816
[35] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2781
[36] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8860
[37] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2741
[38] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2523
[39] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[40] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[41] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2690
[42] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2834
[43] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2861
[44] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2615
[45] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2698
[46] http://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=10554
[47] https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313
[48] https://gzk.rks-gov.net/ActDetail.aspx?ActID=51618

9. UDHËZIMET MBI ZBATIMIN, MONITORIMIN DHE RAPORTIMIN

Udhëzimet e mëposhtme janë hartuar për të ndihmuar dhe udhëzuar të gjitha ministritë që t'i zbatojnë masat individuale në mënyrë efikase

1. ***Siguria:*** Operimi dhe zhvillimi i mëtejshëm i sistemeve të TI-së duhet të bazohet në një filozofi sigurie gjithëpërfshirëse që përfshin elemente strategjike, organizative dhe teknike, siç është siguria sipas dizajnit (security by design). Për këtë duhet të hartohet një qasje e përbashkët për të gjitha institucionet.
2. ***Një qasje e bazuar në rrezik***: Strategjia bazohet në një qasje gjithëpërfshirëse dhe të bazuar në analizën e rrezikut që synon të identifikojë dhe t'i japë përparësi rreziqeve më të

mundshme dhe më serioze, dhe të zhvillojë kundërmasa të përshtatshme për t'u marrë me ato,

3. ***Një qasje shumë-palëshe:*** Si pjesë e qasjes bashkëpunuese, të gjithë akterët përkatës duhet të përfshihen në diskutime dhe t'u jepet mundësia për të ndikuar në proceset dhe aktivitetet sa herë që është e mundur. Është veçanërisht e rëndësishme të sigurohet që masat e marra në sektorin publik dhe privat janë komplementare.
4. ***Përputhshmëria me BE-në***: Prioritetet dhe zhvillimet në nivel të Bashkimit Evropian duhet të merren parasysh gjatë zbatimit të masave.

Këshilli Shtetëror i Sigurisë Kibernetike kryen monitorimin sistematik dhe koordinimin e zbatimit të Strategjisë Kombëtare të Sigurisë Kibernetike, duke marrë parasysh të gjitha sfidat ekzistuese dhe të ardhshme në fushën e sigurisë kibernetike.

Monitorimi i implementimit të objektivave dhe aktiviteteve të planit të veprimit do të bëhet duke u bazuar në këto elemente kyçe:

- Do të hartohet raporti periodik i progresit për realizimin e objektivave të strategjisë dhe zbatimin e planit të veprimit.
- Do të hartohet raporti vjetor i progresit që do të ofrojë informata mbi progresin kundrejt objektivave të zbatimit të aktiviteteve. Vëmendje e veçantë do t'i kushtohet analizës së pengesave, sfidave dhe rreziqeve në lidhje me zbatimin e strategjisë.
- Institucionet pjesëmarrëse do të ofrojnë informata mbi zbatimin e aktiviteteve strategjike për të cilat kanë përgjegjësi udhëheqëse.
- Objektivat me kosto të ulët dhe me ndikim të lartë duhet të kenë prioritet mbi të gjitha përpjekjet.

Përgjegjësia për monitorimin e zbatimit të Strategjisë është e Këshillit Shtetëror të Sigurisë Kibernetike. Procesi i zbatimit të strategjisë duhet të jetë transparent, i hapur dhe i shoqëruar me mbikëqyrje demokratike.

Sekretariati i Strategjive ruan të gjitha planet e zbatimit dhe i përdor ato si bazë për raportin e progresit.

Strategjia do t'i nënshtrohet vlerësimit të ndërmjetëm në vitin 2025 për të vlerësuar efektivitetin dhe efikasitetin e zbatimit. Vlerësimi përfundimtar do të bëhet në vitin 2027.

- Monitorimi i aktiviteteve me të cilin përcaktohet nëse aktivitetet janë kryer në kohën e duhur dhe në cilësinë e duhur. Mjeti kryesor për monitorimin e aktiviteteve është plani i veprimit, i cili përcakton kalendarin e zbatimit për çdo aktivitet. Sa herë që aktivitete të ndryshme devijojnë nga programi i tyre, duhet të kontrollohet nëse ka pasoja për aktivitete dhe burime të

tjera. Arsyet e devijimeve të tilla duhet të analizohen, ndërsa plani i zbatimit duhet të korrigjohet në aspektin kohor.

Monitorimi i objektivave bazohet në treguesit e tyre. Treguesit kanë vlerën bazë, synimin e ndërmjetëm dhe për vitin e fundit në përputhje me periudhën e dokumentit strategjik. Që monitorimi të jetë efektiv, duhet të vendosen synime të ndërmjetme në baza vjetore, duke u bërë pjesë e planit vjetor të punës. Më pas nxirret përfundimi duke krahasuar vlerën aktuale me qëllimin e synuar.

Megjithatë, përcaktimet dhe metodologjitë e sakta për llogaritjen e treguesve nuk janë finalizuar përpara miratimit të kësaj strategjie. Pra, të gjithë treguesit e parashikuar në strategjinë kombëtare për sigurin kibernetike 2023-2027 dhe planin e saj të veprimit duhet të konsiderohen sygjerime indikative. Lista e saktë dhe përshkrimi i treguesve, metodologjia e matjes së tyre, vlerat bazë dhe objektivat do të përcaktohen në Pasaportën e Treguesve, e cila do të finalizohet brenda 3 muajve nga miratimi i kësaj strategjie.