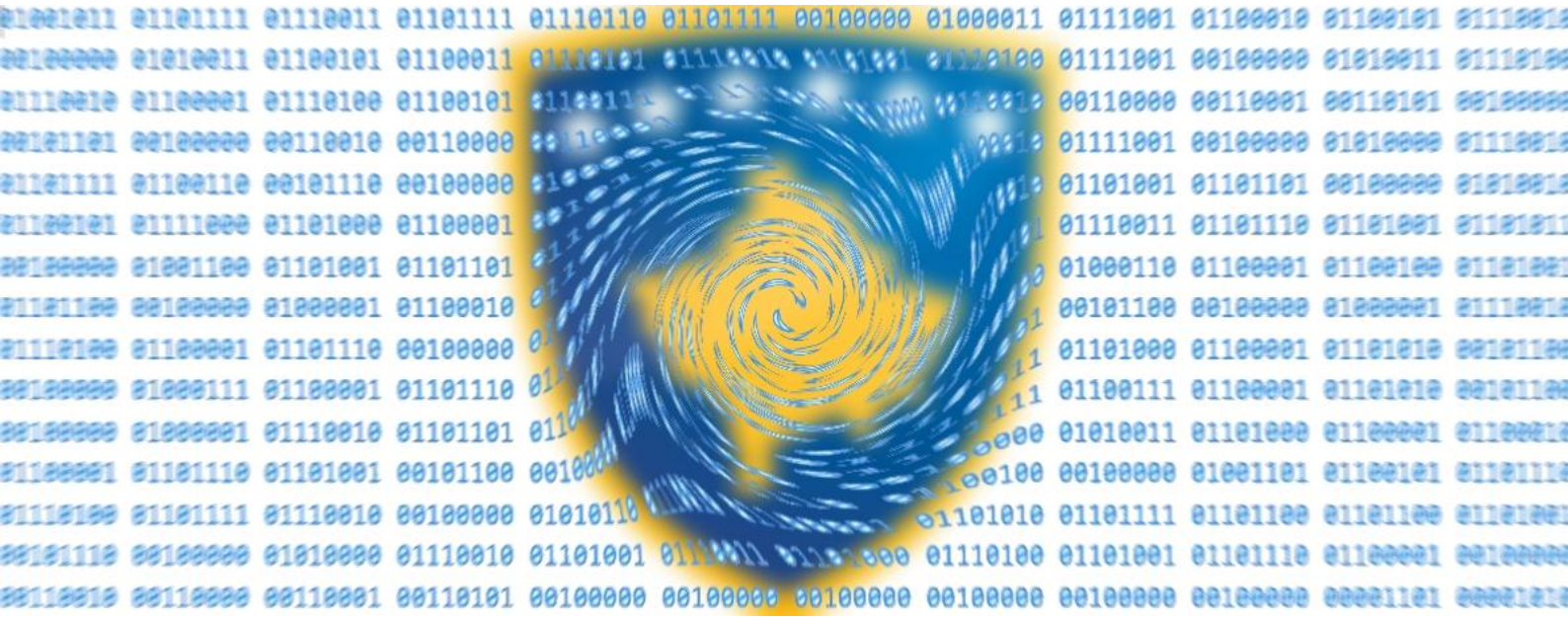
REPUBLIKA E KOSOVËS
REPUBLIKA KOSOVA / REPUBLIC OF KOSOVO

QEVERIA E KOSOVËS
VLADA KOSOVA / GOVERNMENT OF KOSOVO

MINISTRIA E PUNËVE TË BRENDSHME
MINISTARSTVO UNUTRAŠNJIH POSLOVA
MINISTRY OF INTERNAL AFFAIRS



Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016 – 2019

Dhjetor 2015

Përmbledhje ekzekutive

Interneti i sotëm me hapësirën kibernetike (virtuale) është sistemi më i madh i krijuar ndonjëherë nga njerëzimi, me miliarda pajisje të lidhura, përmes lidhjeve të shumta komunikuese, e me miliarda përdorues që lidhen me laptopë, tabletë, si dhe telefona të mençur. Prirja është që secili dhe çdo gjë të lidhet, ndërsa ky trend ka prirje të shkojë drejt rritjes së mëtutjeshme. Sipas Statistikave Botërore të Internetit (Internet World Stats) rritja e përdorimit të Internetit për periudhën 2000-2014 ka qenë 741%, ndërsa penetrimi i Internetit në nivel global rreth 42%. Ndërsa, sipas Gartner Inc., deri më 2020 do të ketë afërsisht 26 miliardë pajisje në Internet. Me këtë përdorim të madh të Internetit, si platformë kryesore e punës, shkencës dhe komunikimit social të qytetarit modern, siguria dhe privatësia e tij kthehen në brenga kryesore.

Interneti me hapësirën e tij kibernetike paraqet një prej shtytësve më të rëndësishëm të inovacionit, rritjes dhe konkurrencës së ekonomive shtetërore në të gjithë botën. Në një botë të globalizuar dhe të ndërlidhur, hapësira kibernetike dhe siguria e saj kthehen si objektiva kyçe strategjike në fushën e sigurisë në secilin vend. Interneti dhe aktivitetet e tij kibernetike, si ato ekonomike, shkencore dhe sociale, po fitojnë përditë e më shumë rëndësi. Kjo liri kibernetike dhe vlerat njerëzore duhen mbrojtur në të njëjtën mënyrë si në botën jashtë Internetit. Infrastruktura digjitale duhet mbrojtur nga incidentet potenciale, keqpërdorimi dhe aktivitetet keqdashëse. Institucionet qeveritare duhet të kenë rolin kryesor, fillimisht duke përcaktuar politika dhe udhëzime të qarta dhe transparente, për të siguruar jo vetëm hapjen dhe përfshirjen e secilit qytetar, por edhe sigurinë e hapësirës kibernetike.

Në Kosovë, përdorimi i teknologjisë së informacionit dhe komunikimit (TIK) është zgjeruar me shpejtësi prej vitit 2000, ndërsa tanimë TIK-u luan rol të rëndësishëm në të gjitha aspektet e jetës sonë. Penetrimi i Internetit në Kosovë është 76.6%, shkallë kjo shumë e ngjashme me mesataren e Bashkimit Evropian (BE), 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. Megjithatë, në të njëjtën kohë, ato u ekspozohen edhe rreziqeve të ndryshme në hapësirën e Internetit. Këto rreziqe qëndrojnë tek cenimi i pashmangshëm në TIK, si dhe mund të shkaktojnë mungesa të shërbimit apo edhe keqpërdorim të shërbimeve, duke rezultuar kështu me dëmtim (humbje) të mundshëm të jetëve të njerëzve, humbje ekonomike në masë të madhe, rrënim të rendit publik si dhe kërcënime ndaj sigurisë shtetërore.

Në këtë kontekst, Qeveria e Republikës së Kosovës ka përfshirë në Programin e Qeverisë 2015-2018 hartimin e Strategjisë Shtetërore për Sigurinë Kibernetike dhe Planin e Veprimit 2016 – 2019, si dhe me Vendimin nr. 01/30 të datës 20.05.2015 ka përfshirë strategjinë në Planin e Dokumenteve Strategjike për vitin 2015. Grupi punues me të gjitha palët e përfshira është themeluar në kuadër të Ministrisë së Punëve të Brendshme (MPB). Ky grup punues ka për mandat të përgatisë politikat, strategjinë dhe planin e veprimit për sigurinë kibernetike në nivel shtetëror. Të gjitha organizatat

dhe agjencitë shtetërore, personat fizik dhe juridik, janë të obliguar të kryejnë detyrat e përcaktuara në kuadër të politikave, strategjive dhe planeve të veprimit të përcaktuara nga Këshilli Shtetëror i Sigurisë Kibernetike.

Strategjia Shtetërore për Sigurinë Kibernetike adreson çështjen e sigurisë kibernetike në Republikën e Kosovës përmes këtyre objektivave strategjik:

1. Mbrojtja e infrastrukturës kritike të informacionit;
2. Zhvillimi institucional dhe ngritja e kapaciteteve;
3. Ndërtimi i partneriteteve publiko-private;
4. Reagimi ndaj incidenteve;
5. Bashkëpunimi ndërkombëtar.

Përmbajtja

Lista e shkurtesave

AKI	Agjencia e Kosovës për Inteligjencë
ARKEP	Autoriteti Rregullativ i Komunikimeve Elektronike dhe Postare
ASHI	Agjencia e Shoqërisë së Informacionit
ASHMDHP	Agjencia Shtetërore për Mbrojtjen e të Dhënave Personale
CERT	Ekipi Reagues për Emergjenca Kompjuterike
CSIRT	Ekipi Reagues për Incidentet e Sigurisë Kompjuterike
ENISA	Agjencia Evropiane për Sigurinë e Rrjeteve dhe Informacionit
IKI	Infrastruktura Kritike e Informacionit
KGJK	Këshilli Gjyqësor i Kosovës
KPK	Këshilli Prokurorial i Kosovës
KSHSK	Këshilli Shtetëror për Sigurinë Kibernetike
MASHT	Ministria e Arsimit, Shkencës dhe Teknologjisë
MD	Ministria e Drejtësisë
MIKI	Mbrojtja e Infrastrukturës Kritike të Informacionit
MF	Ministria e Financave
MFSK	Ministria për Forcën e Sigurisë së Kosovës
MIE	Ministria e Integrimit Evropian
MPB	Ministria e Punëve të Brendshme
MPJ	Ministria e Punëve të Jashtme
MZHE	Ministria e Zhvillimit Ekonomik
OSBE	Organizata për Siguri dhe Bashkëpunim në Evropë
PK	Policia e Kosovës
SKI	Sistemet e Komunikimit dhe të Informacionit
STIKK	Shoqata e Teknologjisë Informative dhe Komunikimit të Kosovës
TIK	Teknologjia e Informacionit dhe Komunikimit

1 Hyrje

1.1 Qëllimi

Qëllimi i këtij dokumenti strategjik është të vendos bazat e përgjithshme të Strategjisë Shtetërore të Sigurisë Kibernetike për tri vitet vijuese në Republikën e Kosovës. Për më tepër, ky dokument paraqet vizionin e Qeverisë së Kosovës për sigurinë kibernetike dhe planin përkatës të veprimit. Strategjia Shtetërore për Sigurinë Kibernetike është pjesë e Programit të Qeverisë 2015-2018, si dhe ndërlidhet me Planin Kombëtar për Zbatimin e Marrëveshjes së Stabilizim Asociimit.

Në këtë epokë globalizimi, pas energjisë, siguria kibernetike është bërë një prej synimeve kryesore strategjike të secilit vend. Revolucioni digjital ka prekur çdo sferë të jetës në botën moderne. Më shumë se kurrë, secili vend po përpiqet të përfitojë nga hapësira kibernetike duke shtyrë përpara zhvillimin ekonomik, shkencor dhe social, por edhe atë politik. Zhvillimi i infrastrukturës digjitale si Interneti ka ndryshuar shumë jetën tonë të përditshme sociale dhe ekonomike.

Liria në Internet dhe vlerat njerëzore duhen mbrojtur në të njëjtën mënyrë si jashtë Internetit. Infrastruktura digjitale duhet mbrojtur nga incidentet potenciale dhe veprimet keqdashëse. Institucionet publike kanë rolin kryesor, fillimisht duke vendosur udhëzime dhe politika të qarta e transparente, për të siguruar jo vetëm hapjen dhe përfshirjen e secilit qytetar, por edhe sigurinë në hapësirën kibernetike.

Më 2013, Shoqata e Teknologjisë Informative dhe Komunikimit (STIKK) botoi një studim për penetrimin dhe përdorimin e Internetit në Kosovë[1]. Sipas këtij studimi, penetrimi i Internetit në bazë të amvisërive është 84.8%, ndërsa në bazë të përdoruesve ai është 76.6%, gjë që është shumë e afërt me mesataren e Bashkimit Evropian (BE). Për më tepër, ky studim thekson që sjelljet e shumicës së kosovarëve në hapësirën e Internetit mund të krahasohen me trendet globale.

Duke iu referuar "*Analizës së rishikimit strategjik të sektorit të sigurisë në Republikën e Kosovës*"[2], krimi kibernetik si krim jokonvencional është identifikuar si një prej rreziqeve, sfidave apo kërcënimeve globale që mund të cenojnë edhe sigurinë e Kosovës.

Republika e Kosovës është zotuar të promovojë stabilitetin dhe sigurinë, jo vetëm brenda vendit, por edhe të jetë kontribuuese e rëndësishme ndaj sigurisë së rajonit dhe më gjerë. Kështu, bashkëpunimi ndërkombëtar në fushën e sigurisë kibernetike mbetet prioritet për Kosovën.

1.2 Vizioni

Republika e Kosovës do të sigurojë një mjedis të sigurt të hapësirës kibernetike, duke minimizuar dhe parandaluar kërcënimet kibernetike në bashkëpunim me partnerët vendorë dhe ndërkombëtarë.

[1]STIKK - http://stikk.org/fileadmin/user_upload/Depertimi_dhe_perdorimi_i_internetit_ne_Kosove_01.pdf
[2]RSSS - http://www.kryeministri-ks.net/repository/docs/Analiza_e_Rishikimit_Strategjik_te_Sektorit_te_Sigurise_se_RKS_06032014.pdf

1.3 Përkufizimi i termave

Në nivel Evropian dhe ndërkombëtar, nuk ka ndonjë definicion të harmonizuar të atyre që quhet "kibernetikë" dhe "siguri kibernetike". Kuptimi i sigurisë kibernetike dhe termave të tjerë të rëndësishëm dallon nga vendi në vend.

Në këtë kapitull, do të paraqiten definicionet e termave specifikë të përafruar me kuptimin themelor të këtyre termave në vendet e BE-së. Qëllimi i kësaj liste është të ngrejë vetëdijen e popullatës në përgjithësi për terminologjinë kompjuterike.

"Kibernetika"(cyber) definohet si: *"çdo gjë që ka të bëjë me, apo që përfshin, kompjuterët apo rrjetet kompjuterike (si Interneti)".*

Sipas Organizatës Ndërkombëtare për Standardizim (ISO), "cyber" është *"mjedis kompleks që lind nga ndërveprimi i njerëzve, i programeve dhe i shërbimeve në Internet, me anë të pajisjeve e rrjeteve teknologjike që lidhen në të, që nuk ekziston në formë fizike".*

Hapësira kibernetike
Hapësira kibernetike është hapësira virtuale e të gjitha sistemeve të TI-së të ndërlidhura në nivel të dhënash në shkallë globale. Baza e hapësirës kibernetike është Interneti, si rrjet universal dhe publikisht i qasshëm për lidhje dhe transportim, i cili mund të plotësohet e zgjerohet tutje për çfarëdo numri të rrjeteve të tjera të të dhënave. Sistemet e TI-së në hapësira të izoluara virtuale nuk janë pjesë e hapësirës kibernetike.

Gjithashtu, dihet që mjedisi global krijohet përmes ndërlidhjes së sistemeve të komunikimit dhe informacionit. Hapësira kibernetike përfshin rrjetet kompjuterike fizike dhe virtuale, sistemet kompjuterike, formatet dhe të dhënat digjitale.

Siguria kibernetike
Në Strategjinë e Sigurisë Kibernetike të Bashkimit Evropian (Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur)[3], "*siguria kibernetike përgjithësisht iu referohet masave mbrojtëse dhe veprimeve që mund të ndërmerren për të mbrojtur domenin kibernetik, edhe në fushën civile edhe atë ushtarake, nga ato kërcënime që ndërlidhen me to apo që mund të dëmtojnë rrjetet dhe infrastrukturën komunikuese të ndërvarura. Siguria kibernetike përpiqet të ruajë disponueshmërinë dhe integritetin e rrjeteve dhe infrastrukturës, si dhe fshehtësinë e informatave që mbahen në to.*"

Organizata Ndërkombëtare e Standardizimit (ISO) përkufizon sigurinë kibernetike si *"ruajtje të konfidencialitetit, integritetit dhe disponueshmërisë së informatave në hapësirën kibernetike".*

Definicionet e tjera e definojnë sigurinë kibernetike si objektiv të dëshiruar të fushës së sigurisë së TI-së, në të cilën rreziqet e hapësirës globale kibernetike ngushtohen deri në një minimum të pranueshëm. Kështu, siguria kibernetike në Kosovë është objektiv i dëshiruar për TI-në, në të cilën rreziqet e hapësirës kibernetike të Kosovës do të zvogëlohen deri në minimumin e pranueshëm.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001

Siguria kibernetike (në Kosovë) është shuma e masave të përshtatshme dhe të duhura. Siguria kibernetike civile fokusohet te të gjitha sistemet e TI-së për përdorim civil në hapësirën kibernetike të Kosovës. Është gjithashtu gjendja e dëshiruar në të cilën mbrojtja e hapësirës kibernetike është proporcionale ndaj kërcënimit kibernetik, si dhe pasojave të mundshme të sulmeve kibernetike.

Kriminaliteti kibernetik

Sipas Strategjisë së lartpërmendur të Sigurisë Kibernetike të Bashkimit Evropian, *"kriminaliteti kibernetik i referohet përgjithësisht një spektri të gjerë veprimtarish kriminale të ndryshme, ku kompjuterët dhe sistemet informative angazhohen ose si vegël primare ose si shënjestër primare. Krimi kibernetik përfshin veprat penale tradicionale (p.sh. mashtrimi, falsifikimi dhe thyerja e identitetit), veprat në lidhje me përmbajtjen (p.sh. shpërndarja në Internet e pornografisë së fëmijëve apo nxitja e urrejtjes racore), si dhe veprat që janë unike për kompjuterë dhe sisteme informative (p.sh. sulmet ndaj sistemeve informative, mohimi i shërbimit dhe maluer (malware))."*

Ai përbëhet nga vepra penale që kryhen në rrjete, me anë të rrjeteve elektronike të komunikimit dhe informimit. Ky është problem i pakufishëm, që mund të klasifikohet në tri definicione më të gjera[4]:

- Krimet specifike të Internetit, si sulmet ndaj sistemeve informative apo phishing (p.sh. faqe të rreme bankare për të marrë fjalëkalime që mundësojnë qasje në llogari bankare të viktimave);
- Mashtrime dhe falsifikime kibernetike: Vjedhja e identitetit, phishing, posta e padëshiruar, klonimi i kartelave bankare dhe kartelave tjera, si dhe kodimet keqdashëse;
- Përmbajtja e paligjshme online, duke përfshirë materialet me keqpërdorim seksual të fëmijëve, nxitjen e urrejtjes racore, nxitjen e akteve terroriste dhe idealizimin e dhunës, terrorizmit, racizmit dhe ksenofobisë.

Sulmet kibernetike, spiunimi kibernetik dhe sabotazhi kibernetik

Sulmi kibernetik është sulm në TI në hapësirën kibernetike, i drejtuar ndaj një apo më shumë sistemeve teknologjike, me qëllim të cenimit të sigurisë së TI-së. Synimet e sigurisë, konfidencialitetit, integritetit dhe disponueshmërisë së TI-së mund të kompromentohen, individualisht apo në grup. Sulmet kibernetike kundër konfidencialitetit të një sistemi TI, të cilat ushtrohen apo menaxhohen nga shërbimet e huaja inteligjente, quhen spiunim kibernetik. Sulmet kibernetike ndaj integritetit dhe disponueshmërisë së sistemeve të TI-së, quhen sabotim kibernetik.

Mbrojtja kibernetike përdoret kryesisht në kontekst ushtarak, por mund të ketë të bëjë edhe me aktivitetet kriminale dhe spiunimin. NATO-ja përdor këtë definicion për shpjegimin e mbrojtjes kibernetike: "aftësia për mbrojtjen e ofrimit dhe menaxhimit të shërbimeve në Sisteme Komunikimi dhe Informacioni (SKI) në përgjigje ndaj veprimeve të mundshme, të afërta por edhe të ndodhura keqdashëse të cilat lindin në hapësirën kibernetike". Mbrojtja kibernetike përbëhet nga këto detyra: Mbrojtje, Zbulim, Reagim dhe Rikuperim.

[4] Komisioni Evropian - http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

Inteligjenca Kibernetike
Veprimtaritë që shfrytëzojnë të gjitha burimet e "inteligjencës" në përkrahje të sigurisë kibernetike, për të identifikuar kërcënimet e përgjithshme kibernetike, për të grumbulluar synimet dhe aftësitë kibernetike të kundërshtarëve të mundshëm, për të analizuar dhe komunikuar, si dhe për të identifikuar, gjetur dhe reaguar ndaj burimeve të sulmeve kibernetike.

Terrorizmi kibernetik është një zgjedhje përditë e më atraktive për terroristë, sepse mund të arrihet me burime modeste financiare, në mënyrë anonime, si dhe nga distanca të mëdha. Terrorizmi kibernetik ka potencialin më të madh për dëmtime kur bashkohet me sulmet e koordinuara fizike. Epiteti *kibernetik* këtu përdoret pasi që terroristi sulmon apo përdor teknologjinë.

Infrastruktura kritike
Infrastrukturë kritike është prona ose institucioni me rëndësi të madhe për të mirën publike, dështimi apo cenimi i të cilave do të qonte drejt tkurrjeve të qëndrueshme të furnizimit, çrregullimeve të konsiderueshme të sigurisë publike, apo pasoja të tjera dramatike.

Në Dokumentin e Gjelbër të Programit Evropian për Mbrojtjen e Infrastrukturës Kritike, Komisioni Evropian jep një listë indikative prej 11 sektorëve kritikë:[5]

- Energjia
- Teknologjia e informacionit dhe komunikimit
- Uji
- Ushqimi
- Shëndetësia
- Financat
- Rendi dhe siguria publike dhe juridike
- Administrata civile
- Transporti
- Industria kimike dhe bërthamore
- Hapësira dhe hulumtimet

Infrastruktura kritike e informacionit (IKI)
Me infrastrukturë kritike të informacionit nënkuptojmë sistemet TIK që janë infrastruktura kritike për vetveten apo që janë thelbësore për funksionimin e infrastrukturave kritike (telekomunikacioni, kompjuterët/softuerët, Interneti, satelitët etj.).

Mbrojtja e infrastrukturës kritike të informacionit (MIKI)
Programet dhe aktivitetet e pronarëve, operatorëve, prodhuesve, përdoruesve dhe autoriteteve rregullatore të infrastrukturës, të cilat kanë për qëllim të ruajnë performancën e infrastrukturave kritike të informacionit në rast të dështimit, sulmit apo aksidenteve mbi një nivel të definuar minimal të shërbimeve, si dhe që synojnë shkurtimin e kohës së rikuperimit dhe tkurrjen e dëmeve.

MIKI pra duhet shikuar si fenomen ndërsektorial, e jo si fenomen që kufizohet te sektorë të veçantë.

[5] Komisioni Evropian – Dokumenti i Gjelbër për Programin Evropian për Mbrojtjen e Infrastrukturës Kritike http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576

MIKI duhet të bashkërendohet ngushtë me mbrojtjen e infrastrukturës kritike nga një këndvështrim i gjithmbarshëm.

Alarmimi
Njoftimi për situata të mundshme fatkeqësish që mund të ndodhin, ekzistojnë apo kanë ngjarë. Udhëzim për pranuesin që të qëndrojë i gatshëm për ndonjë eskalim të mundshëm apo aktivizim të masave përkatëse.

Ekipi Reagues ndaj Incidenteve të Sigurisë Kompjuterike
Ekipi reagues për incidentet e sigurisë kompjuterike apo shkurtimisht CSIRT është organizatë shërbyese përgjegjëse për pranimin, shqyrtimin dhe reagimin ndaj incidenteve dhe aktiviteteve të tjera kundër sigurisë kompjuterike. Shërbimet e saj zakonisht përcaktohen për një institucion të përkufizuar që mund të jetë subjekt amë, si organizatë, korporatë, qeveritare apo arsimore, rajon apo vend, rrjet hulumtues, ose një klient i paguar.

CSIRT-i mund të jetë ekip zyrtar apo ekip *adhoc*. Ekipi formal kryen punë të reagimit ndaj incidenteve si funksion kryesor të punës. Ekipi *adhoc* mblidhet gjatë një incidenti të sigurisë kompjuterike në vijim apo për të reaguar sipas nevojës.

Ekipet reaguese ndaj emergjencave kompjuterike
Ekipet reaguese ndaj emergjencave kompjuterike apo shkurtimisht CERT janë grupe ekspertësh që merren me incidentet e sigurisë kompjuterike. Emërtime të tjera për grupe të tilla mund të jenë ekipet e gatishmërisë për emergjenca kompjuterike dhe ekipe reaguese ndaj incidenteve të sigurisë kompjuterike (CSIRT).

Titulli "Ekip Reagues ndaj Emergjencave Kompjuterike" është përdorur së pari nga Qendra Koordinuese CERT (CERT-CC) në Universitetin Carnegie Mellon (CMU). Shkurtesa CERT e emërtimit historik pastaj u përdor nga ekipet e ngjashme në gjithë botën.

Agjencia Evropiane për Sigurinë e Rrjeteve dhe Informacionit (ENISA)
Agjencia Evropiane për Sigurinë e Rrjeteve dhe Informacionit (ENISA) është agjenci e Bashkimit Evropian (BE), e krijuar për parandalimin dhe adresimin e problemeve në sigurinë e rrjeteve dhe sigurinë e informatave.

2 Metodologjia

Strategjia Shtetërore për Sigurinë Kibernetike është hartuar duke u bazuar në vlerësimet dhe analizat e agjencive të zbatimit të ligjit, institucioneve qeveritare dhe organizatave vendore dhe ndërkombëtare, trendëve globale, si dhe praktikave dhe politikave të Bashkimit Evropian. Në këtë kontekst, Strategjia është në harmoni të plotë me udhëzimet e ENISA dhe strategjitë e shteteve anëtarë të BE-së.

Grupi i Punës për hartimin e Strategjisë është formuar nga Ministri i Ministrisë së Punëvë të Brendshme me Vendimin Nr. 195/2015 të datës 05.06.2015 ku janë të përfshira të gjitha institucionet shtetërore, shoqatat profesionale, sektori privat, shoqëria civile dhe partnerët ndërkombëtarë.

Në takimin e parë të Grupit Punues është caktuar një grup i ngushtë për të hartuar draftin fillestar të Strategjisë. Ky nëngrup ka mbajtur disa takime dhe ka hartuar draftin fillestar i cili iu është përcjellë të gjithë anëtarëve. Strategjia është hartuar duke siguruar transparencë të plotë dhe përfshirje të të gjithë anëtarëve dhe përfaqësuesve të institucioneve.

Strategjia është hartuar duke aplikuar metodën krahasimore, fillimisht duke analizuar ngjashmëritë dhe ndryshimet e sigurisë kibernetike të Kosovës me shtetet tjera rajonale dhe shteteve tjera. Në bazë të kësaj analize janë identifikuar masat aktuale dhe atyre që duhen të ndërmerren për të krijuarr një mekanizëm efektiv dhe në harmoni me trendet globale për të garantuar sigurinë kibernetike në Republikën e Kosovës.

Është analizuar poashtu literatura teorike dhe empirike në fushën e sigurisë kibernetike dhe janë përdorur si materiale bazë burimet primare dhe sekondare si: analizat dhe vlerësimet e riskut nga institucionet shtetërore, publikimet e ndryshime të organizatave vendore dhe ndërkombëtare, strategjitë e adaptuara të shteteve anëtarë të BE-së, udhëzimet e ENISA-së dhe dokumentet tjera relevante.

Nga 21-23 tetor 2015, është mbajtur punëtoria në Bogë e mbështetur nga Projekti ENCYSEC i financuar nga BE, ku janë ftuar të gjitha institucionet përkatëse. Të gjithë përfaqësuesit kanë pasur mundësinë që të ofrojnë propozimet e tyre dhe diskutojnë mbi Strategjinë dhe aktivitetet e Planit të Veprimit.

3 Sistemi i Menaxhimit të Sigurisë Kibernetike

3.1 Cikli jetësor i Strategjisë

Në bazë të rekomandimeve kyçe të organeve ndërkombëtare (NATO, ENISA), Strategjia Shtetërore për Sigurinë Kibernetike duhet të hartohet brenda një cikli jetësor, i cili përfshin fazat vijuese:

1. Zhvillimi;
2. Zbatimi;
3. Vlerësimi;
4. Përshtatja e Strategjisë.

Kjo mënyrë siguron përparim të vazhdueshëm të Strategjisë, procedurave dhe produkteve, si dhe në përputhje me ndryshimin e rrethanave në mjedisin e afërt dhe më të gjerë.

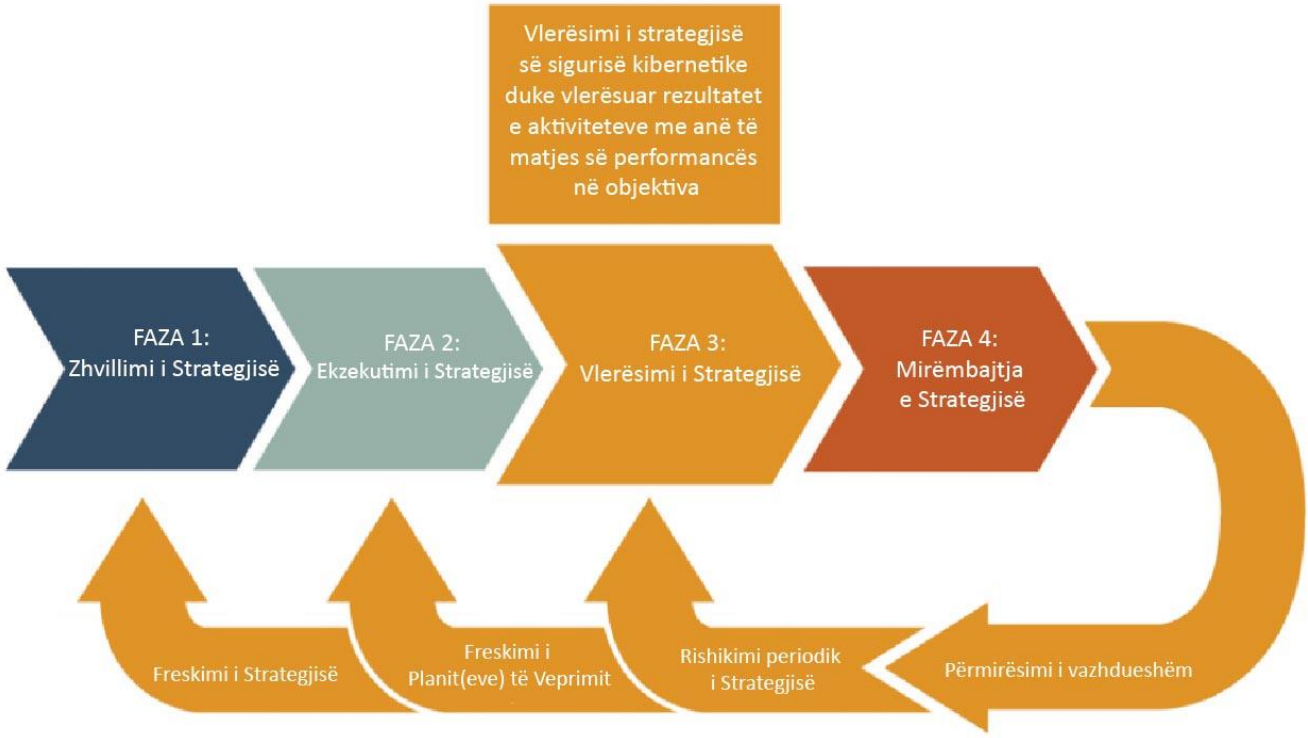


Figura1: Cikli jetësor i sigurisë kibernetike (Burimi: ENISA, 2012)

3.2 Sfidat, rreziqet, kërcënimet ndaj sigurisë së hapësirës kibernetike në Kosovë

Duke marrë parasysh që hapësira kibernetike është hapësirë për keqpërdorime të mundshme kriminale, ka një numër rreziqesh dhe kërcënimesh që cenojnë sigurinë e njerëzve në hapësirën kibernetike të Republikë së Kosovës.

Shumë nga rreziqet dhe ndikimet e incidenteve kibernetike janë të përbashkëta për Qeverinë e Republikës së Kosovës dhe sektorin privat. Synimi i Strategjisë është që të zbuten rreziqet ndaj sigurisë kibernetike, si dhe të mos tolerohen ato rreziqe që kanë ndikim tejet të lartë.

Rreziqet dhe elementet kërcënuese primare që kanë të bëjnë me sistemet e TIK-ut në Republikën e Kosovës janë si më poshtë:

Kërcënimet
Kërcënimet kibernetike vijnë nga mundësitë dhe qëllimet e një armiku që të fillojë një sulm kibernetik mbi Sistemet e Komunikimit dhe të Informacionit.

Ekzistojnë pesë lloje sulmesh kibernetike të motivuara nga:

- **Hakmarrja, kurioziteti:** Të kryera nga stafi brenda organizatës ose ish-të punësuar (të larguar nga puna) dhe nga të ashtuquajtur "script-kiddies" (të rinjë që përdorin skripta të gatshme për sulme);
- **Përfitime monetare:** Të kryera nga krimi i organizuar;
- **Spiunimi, aktivizmi:** Sulmet kibernetike që kanë të bëjnë me ndërhyrjen e pavërejtur të një pale të tretë brenda Sistemeve të Komunikimit dhe të Informacionit, duke lexuar, ndryshuar, shlyer 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;
- **Siguria Kombëtare:** Të kryera nga akterë të sponsorizuar shtetërorë;
- **Terrorizmi:** Terrorizmi kibernetik ka të bëjë me përpjekje me shënjestra të nivelit të lartë, që bëhen me 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.

Infrastruktura kritike e informacionit është në vazhdimësi shënjestër e sulmeve kibernetike. Këto sulme veçanërisht shënjestrojnë caqe specifike të zgjedhura nga terroristët dhe hakerët që kërkojnë informata të ndjeshme apo me qëllim që t'a shkatërrojnë këtë infrastrukturë kritike.

Rreziqet

- Mungesa e Këshillit Shtetëror të Sigurisë Kibernetike me funksionet e tij;
- Mosrreshtimi i CERT-it shtetëror dhe CERT-ve tjerë në Trusted Introducer[6]dhe FIRST[7];
- Mungesa e njohurive dhe e kuptimit të mundësive për sulme kibernetike që përbën rrezik real.

Cenueshmëria
Nuk ekziston siguri dhe mbrojtje e duhur në hapësirën kiberntike. Megjithatë, mundësia e sulmeve kibernetike është shumë më e madhe sesa ajo e sulmit fizik. Autoritetet dhe qytetarët e rëndomtë të

[6]Lista e CERT-ve/CSIRT-ve në Trusted Introducer - https://www.trusted-introducer.org/directory/country_LICSA.html
[7]Lista e anëtarëve të FIRST-it - https://www.first.org/members/teams

Kosovës tashmë kanë qenë viktima të sulmeve kibernetike, dhe sigurisht që edhe do të përballen me sulme të tilla në të ardhmen.

Një prej sfidave më të mëdha gjendet tek rritja e vetëdijes të shfrytëzuesve pasi që shumica e tyre përdorin hapësirën kibernetike. Sipas statistikave botërore, shumica e incidenteve kibernetike shkaktohen për shkak të gabimit njerëzor. Si rezultat, edhe kërcënimi i brendshëm është shumë real.

Përkundër ndikimit të kufizuar të drejtpërdrejtë, rreziqet që kanë të bëjnë me sulmet kibernetike nuk mund të nënvlerësohen.

3.3 Adresimi i krimit kibernetik

Nevoja për bashkëpunim të ngushtë ndërmjet agjencive të zbatimit të ligjit në gjithë botën është urgjente, në mënyrë që të luftohet rritja e shpejtë e krimit kibernetik.

Krimi kibernetik do të jetë një prej sfidave për institucionet e Republikës së Kosovës në të ardhmen e afërt. 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, që në Kosovë është fenomen relativisht i ri.

Rritja e konsiderueshme e numrit të shfrytëzuesve të Internetit në vitet e fundit në Kosovë 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 në vend të cilat ende konsiderohen që janë në fazën e zhvillimit.

Sipas të dhënave në dispozicion, shënjestra kryesore e sulmeve kibernetike në Kosovë deri më sot kanë qenë llogaritë e shfrytëzuesve, sistemi bankar, dhe ueb faqet në Internet.

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 avancohet mekanizmi në Policinë e Kosovës 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 policisë në mënyrë që të avancohen kapacitetet e Policisë së Kosovës në ndjekje të krimit kibernetik.

Krimi kibernetik kërkon reagim të specializuar të institucioneve dhe agjencitë e zbatimit të ligjit duhet të jenë në gjendje të ndërmarrin hetime dhe të përndjekin veprat kundër të dhënave dhe sistemeve kompjuterike, veprat e kryera përmes kompjuterit, si dhe dëshmitë elektronike të ndërlidhura me veprat penale.

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

4 Parimet e përgjithshme

Struktura dhe përmbajtja e këtij dokumenti bazohet në këto parime:

Parimi i kushtetutshmërisë dhe ligjshmërisë - veprimet e ndërmarra për të avancuar sigurinë kibernetike duhen bazuar në dispozitat e parapara me Kushtetutën e Republikës së Kosovës, legjislacionit në fuqi dhe marrëveshjet ndërkombëtare.

Parimi i sigurisë shtetërore – siguria kibernetike është pjesë përbërëse e sigurisë shtetërore, mbështet funksionimin e shtetit dhe shoqërisë, konkurrueshmërinë së ekonomisë dhe inovacionin. Ky parim nënkupton mbrojtjen e të drejtës për siguri dhe mbrojtje për të gjithë qytetarët, përmes parandalimit të krimit kibernetik.

Parimi i përgjegjësisë – për shkak të pronësisë dhe funksionimit të larmishëm të sistemeve të ndryshme të TIK, shteti nuk mund të mbajë përgjegjësinë si i vetëm për mbrojtjen e hapësirës kibernetike dhe të të drejtave të qytetarëve në Internet. Pronarët dhe operatorët e TIK-ut kanë përgjegjësi primare për mbrojtjen e sistemeve të tyre, si dhe të informatave të përdoruesve të tyre.

Parimi i qasjes së gjithmbarshme - është qenësore të zhvillohet një qasje e gjithmbarshme në përballje me kërcënimet në hapësirën kibernetike.

Parimi i partneritetit publiko-privat – siguria kibernetike mundësohet në mënyrë të bashkërenduar përmes bashkëpunimit ndërmjet sektorit privat dhe atij publik, duke marrë parasysh ndërlidhjen dhe ndërvarësinë e infrastrukturës dhe të shërbimeve ekzistuese në hapësirën kibernetike.

Parimi i vazhdimësisë – aktivitetet duhen parë si pjesë e një strategjie të vazhdueshme. Kjo ka rëndësi të veçantë sepse do të ketë afate administrative, procedurale dhe kohore, si dhe për shkak se iniciativat e veprimet e ndryshme duhen ndërlidhur me veprimet që do të vazhdojnë për vite me radhë.

Parimi i konfidencialitetit – institucionet me përgjegjësi në parandalimin dhe luftimin e krimit kibernetik duhet të krijojnë besimin tek mbrojtja e hetimeve, të dhënave dhe integritetit të informatave nga keqpërdorimi nga ata që kanë qasje në to.

Parimi i të drejtave dhe lirive të njeriut – siguria kibernetike garantohet duke respektuar të drejtat dhe liritë themelore, si dhe duke mbrojtur liritë individuale, informatat personale, si dhe identitetin, pa marrë parasysh etninë, gjininë, moshën, fenë dhe orientimin seksual.

Parimi i bashkëpunimit ndërkombëtar – siguria kibernetike avancohet përmes bashkëpunimit ndërkombëtar me partnerë dhe aleatë. Përmes bashkëpunimit, Republika e Kosovës do të luajë rol qenësor në promovimin e sigurisë kibernetike globale.

5 Korniza ligjore dhe mekanizmat institucional

5.1 Korniza ligjore

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

- Kushtetuta e Republikës së Kosovës[8];
- Ligji nr. 03/L-050 për Themelimin e Këshillit të Sigurisë së Kosovës[9];
- Ligji nr.03/L –166 për Parandalimin dhe Luftimin e Krimit Kibernetik[10];
- Ligji nr. 04/L-145 për Organet Qeveritare të Shoqërisë së Informacionit[11];
- Ligji nr. 04/L-094 për Shërbimet e Shoqërisë Informatike[12];
- Ligji nr. 04/L-109 për Komunikimet Elektronike[13];
- Ligji nr.05/L-030 për Përgjimin e Komunikimeve Elektronike[14];
- Ligji nr.03/L – 172 për Mbrojtjen e të Dhënave Personale[15];
- Ligji nr. 04/L-076 për Policinë[16];
- Ligji nr. 03/L-142 për Rendin dhe Qetësinë Publike[17];
- Ligji nr. 03/L063 për Agjencinë e Kosovës për Inteligjencë[18];
- Ligji nr. 04/L-149 për Ekzekutimin e Sanksioneve Penale[19];
- Ligji nr. 04/L-065 për të Drejtën e Autorit dhe të Drejtat e Përafërta[20];
- Ligji nr. 03/ L-183 për Zbatimin e Sanksioneve Ndërkombëtare[21];
- Ligji nr. 04/L-213 për Ndihmën Juridike Ndërkombëtare në Çështje Penale[22];
- Ligji nr. 04/L-052 për Marrëveshjet Ndërkombëtare[23];
- Ligji nr. 04/L-072 për Kontrollin dhe Mbikëqyrjen e Kufirit Shtetëror[24];
- Ligji nr. 04/L-093 për Bankat, Institucionet Mikrofinanciare dhe Institucionet Financiare Jobankare[25];
- Ligji nr. 04/L-064 për Agjencinë e Kosovës për Forenzikë[26];
- Ligji nr. 04/L-198 për Tregtinë e Mallrave Strategjike[27];
- Ligji nr.04/L –004 për Shërbimet Private të Sigurisë[28];

[8] http://gzk.rks-gov.net/ActDetail.aspx?ActID=3702
[9] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2521
[10] http://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2682
[11] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8669
[12] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2811
[13] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851
[14] https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968
[15] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2676
[16] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2806
[17] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2651
[18] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2538
[19] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8867
[20] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2787
[21] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2674
[22] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8871
[23] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2789
[24] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2801
[25] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2816
[26] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2781
[27] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8860
[28] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2741

- Ligji nr. 03/L-046 për Forcën e Sigurisë së Kosovës[29];
- Kodi nr. 03/L-109 Doganor dhe i Akcizës i Kosovës[30];
- Ligji nr. 04/L-099 për Ndryshim-Plotësimin e Kodit Doganor dhe të Akcizave në Kosovë, nr. 03/l-109[31];
- Ligji nr.03/L-178 për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë[32];
- Kodi nr. 04/L-082 Penal i Republikës së Kosovës[33];
- Kodi nr. 04/L-123 i Procedurës Penale[34];
- Ligji nr.03/L-122 për Shërbim të Jashtëm të Republikës së Kosovës[35];
- Kodi nr.03/L-193 i Drejtësisë për të Mitur[36];
- Rregullore nr.18/2011 për Shpërndarjen dhe Transferimin e Informacionit të Klasifikuar[37].

Kjo strategji është në përputhje me aktet ndërkombëtare që rregullojnë fushën e sigurisë kibernetike, Strategjinë e Sigurisë Kibernetike të Bashkimit Evropian "Hapësirë e hapur, e sigurt dhe e mbrojtur kibernetike (2013)"[38]; Udhëzuesin e ENISA për Strategjitë Shtetërore të Sigurisë Kibernetike (2012)[39]; Strategjitë e Sigurisë Kibernetike të vendeve të tjera të BE-së.

5.2 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 institucione:

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 Strategjinë për Sigurinë 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 përkrahur kështu Planin e Veprimit për Sigurinë Kibernetike.

[29] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2523
[30] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[31] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[32] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2690
[33] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2834
[34] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2861
[35] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2615
[36] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2698
[37] http://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=10554
[38] Strategjia e Sigurisë Kibernetike të Bashkimit Evropian http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[39] Enisa http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Ministria e Punëve të Brendshme
MPB ka rolin kryesor në koordinimin e Strategjisë, monitorimin e zbatimit të Planit të Veprimit, si dhe hartimin e raporteve periodike. MPB po ashtu është përgjegjëse për hartimin dhe monitorimin e politikave dhe legjislacionit në fushën e sigurisë së përgjithshme dhe sigurisë kibernetike. 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, përmes Sektorit për Krimet Kibernetike dhe strukturave tjera mbështetëse në kuadër të Policisë së Kosovës. PK gjithashtu do të shërbejë edhe si Pikë e Përhershme e kontaktit 24/7 për bashkëpunim ndërkombëtar në fushën e krimit kibernetik.

Këshilli Gjyqësor i Kosovës
Siguron që gjykatat në Kosovë të jenë të pavarura, profesionale dhe të paanshme, me qëllim që sistemi gjyqësorë 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 kryesve, 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 Këshillit të Sigurisë së Kosovës.

Agjencia e Kosovës për Inteligjencë
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 përgatit dhe zhvillon legjislacionin në fushën e drejtësisë, si dhe koordinon dhe zhvillon bashkëpunimin juridik ndërkombëtar në çështjet penale.

Ministria për Forcën e Sigurisë së Kosovës
MFSK zhvillon dhe fuqizon mbrojtjen kibernetike për sistemet e komunikimit dhe informacionit të MFSK-së/FSK-së, të cilat sisteme përdoren për kryerjen e detyrave në përmbushje të misonit

kushtetues. FSK mund të angazhohet në mbështetjen e autoriteteve civile në mbrojtjen e të dhënave dhe infrastrukturës kritike në rast të ndonjë krize në vend.

Ministria e Zhvillimit Ekonomik
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 informative dhe të inovacioneve, përkrah qasjen në teknologji për të gjithë qytetarët e Kosovës dhe nxit zhvillimin e sistemeve të aftësimit në teknologjinë informative.

Ministria e Financave
MF 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 dhe Teknologjisë
MASHT luan 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
MPJ ka rol në drejtim të dhënies së ndihmës për bashkëpunim ndërkombëtarë në luftën kundër krimit të organizuar.

Ministria e Integrimit Evropian
MIE siguron që korniza ligjore dhe politikat e Qeverisë së Republikës së Kosovës janë në harmoni me legjislacionin dhe politikat e BE-së.

Autoriteti Rregullativ i Komunikimeve Elektronike dhe Postare
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 Shoqërisë së Informacionit
ASHI bën koordinimin, udhëheqjen dhe mbikëqyrjen e proceseve dhe të mekanizmave të qeverisjes elektronike në lidhje me infrastrukturën e TIK, zgjerimin e shërbimeve të internetit dhe të përmbajtjeve 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.

Agjencia Shtetërore për Mbrojtjen e të Dhënave Personale

ASHMDHP 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.

6 Objektivat e Strategjisë së Sigurisë Kibernetike

Strategjia Shtetërore për Sigurinë Kibernetike ka këto objektiva strategjik:

1. Mbrojtja e infrastrukturës kritike të informacionit;
2. Zhvillimi institucional dhe ngritja e kapaciteteve;
3. Ndërtimi i partneritetit publiko-privat;
4. Reagimi ndaj incidenteve;
5. Bashkëpunimi ndërkombëtar.

6.1 Mbrojtja e Infrastrukturës kritike të informacionit

Kjo Strategji synon të krijojë një mjedis të sigurt të hapësirës kibernetike në Republikën e Kosovës, me masat dhe veprimet specifike për mbrojtjen e infrastrukturës kritike të informacionit, çrregullimi apo shkatërrimi i të cilave do të kishin pasoja të rënda ndaj funksioneve vitale shoqërore.

Mbrojtja e infrastrukturës kritike të informacionit do të jetë pjesë përbërëse e Ligjit për Identifikimin dhe Mbrojtjen e Infrastrukturës Kritike i cili do të hartohet në vitin 2016. Sektori publik dhe ai privat duhet të krijojnë një bazë të avancuar strategjike dhe organizative të bazuar në shkëmbim të intensifikuar informatash. Aty ku është e nevojshme, si dhe në rast të kërcënimeve specifike, masat mbrojtëse do të jenë të detyrueshme. Për më tepër, do të vlerësohet edhe domosdoshmëria e harmonizimit të rregullave për mirëmbajtjen e infrastrukturave kritike gjatë krizave teknologjike.

6.1.1 Identifikimi i infrastrukturës kritike të informacionit

Është e domosdoshme të identifikohet dhe të vlerësohet infrastruktura kritike e informacionit brenda Republikës së Kosovës për mbrojtjen më të mirë të mundshme. Infrastruktura kritike e informacionit do të identifikohet dhe vlerësohet në bazë të një numri të kritereve të përcaktuara, duke marrë parasysh dokumentin e *metodologjive të* ENISA-s *për identifikimin e aseteve dhe shërbimeve të Infrastrukturës Kritike të Informacionit*[40].

Hapat në vijim do të ndiqen për identifikimin e infrastrukturës kritike të informacionit:

- **Përcaktimi i aseteve** që do të trajtohen (p.sh. komunikimet zanore, komunikimet e të dhënave, ruajtja e të dhënave, përpunimi i të dhënave) që mund të klasifikohen si kritike;
- **Identifikimi i infrastrukturës** që është teknikisht e domosdoshme për funksionimin e këtyre shërbimeve;
- **Vendosja e kritereve objektive** për nivelin e mbrojtjes së nevojshme për secilin element të infrastrukturës, me kategorizimin e infrastrukturave dhe shfrytëzimin e kritereve, si numri i përdoruesve të prekur, niveli i ndjeshmërisë së informatave që koncentrohen, ruhen, transmetohen apo përpunohen në ato infrastruktura etj.;
- **Kontrollimi i kritereve** me zhvillimin e skenarëve që marrin parasysh çrregullimin e funksionimit të infrastrukturës së përzgjedhur, brenda kufijve të aktiviteteve të rregullta.

[40]ENISA https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis

6.2 Zhvillimi institucional dhe ngritja e kapaciteteve

6.2.1 Caktimi i Koordinatorit Nacional dhe detyrat e Këshillit Shtetëror për Sigurinë Kibernetike

Pasi që qasja ndaj masave të sigurisë është e shumëanshme, është me rëndësi të kuptohet dhe të pranohet që ruajtja e niveleve të pranueshme të sigurisë në hapësirën kibernetike mund të arrihet vetëm përmes bashkëpunimit ndërmjet palëve të ndryshme të përfshira, në kuadër të një reagimi të koordinuar ndaj kërcënimeve të ndryshme që tashmë janë përmendur në kapitullin 3.

Koordinimi i autoriteteve kompetente apo përkatëse qeveritare është absolutisht i domosdoshëm. Ky koordinim është produktiv kur bëhet nga një subjekt që është në pozitë për të organizuar dhe për të bashkërenduar akterët dhe veprimet e ndryshme në Republikën e Kosovës, për reagim korrekt ndaj kërcënimeve që paraqiten sot, si dhe ndaj kërcënimeve të reja në hapësirën kibernetike.

Këshilli Shtetëror i Sigurisë Kibernetike duhet themeluar për të përforcuar bashkëpunimin brenda autoriteteve publike dhe bashkëpunimit ndërmjet autoriteteve publike me sektorin privat, si dhe për të ofruar rekomandime për çështjet strategjike në nivele të larta politike.

Këshilli përbëhet nga përfaqësuesit e institucioneve vijuese: Ministria e Punëve të Brendshme, Policia e Kosovës, Agjencia e Kosovës për Forenzikë, Ministria e Forcës së Sigurisë së Kosovës, Agjencia e Kosovës për Inteligjencë, Agjencia e Shoqërisë së Informacionit, Këshilli i Sigurisë së Kosovës, Ministria e Drejtësisë, Këshilli Prokurorial i Kosovës, Këshilli Gjyqësor i Kosovës, Ministria e Financave, Dogana e Kosovës, Ministria e Arsimit, Shkencës dhe Teknologjisë, Ministria e Punëve të Jashtme, Autoriteti Rregullator për Komunikimet Elektronike dhe Postare, Banka Qendrore e Kosovës. Në raste të veçanta, do të përfshihen edhe ministritë, agjencitë dhe institucione tjera.

Përfaqësuesit e bizneseve do të ftohen si anëtarë sipas nevojës. Përfaqësues akademik gjithashtu do të angazhohen në nivel teknik. Këshilli Shtetëror për Sigurinë Kibernetike synon të bashkërendojë mjetet parandaluese dhe qasjet ndërdisiplinore të sigurisë kibernetike në sektorin publik dhe atë privat.

6.2.2 Ngritja e kapaciteteve në Sekretariatin e Strategjive

Në mënyrë që të sigurohet monitorimi dhe koordinimi i aktiviteteve të Strategjisë është e domosdoshme që të rekrutohet një Zyrtar në Sekretariatin e Strategjive. Ministria e Punëve të Brendshme deri në kuartalin e tretë të vitit 2016 do të përfundoj të gjitha procedurat e shpalljes dhe rekrutimit të zyrtarit përgjegjës.

Gjithashtu, me mbështetje të partnerëve ndërkombëtarë do të organizohen trajnime dhe vizita studimore me qëllim të ngritjes së kapaciteteve të zyrtarit përkatës.

6.2.3 Vetëdijesimi

Do të punohet për promovimin e një kulture të sigurisë kibernetike në të gjithë shoqërinë, duke përfshirë këtu edhe bashkëpunimin me sistemin arsimor, industrinë, si dhe promovimin e organizimeve si "Muaji Evropian i Sigurisë Kibernetike". Vëmendje e veçantë duhet kushtuar

zyrtarëve qeveritarë, gjeneratave të reja, si dhe përdoruesve të Internetit dhe ofrimit të vazhdueshëm të programeve të reja për sigurinë e informatave në të gjitha nivelet e arsimit, me qëllim të përdorimit të sistemeve të avancuara informative.

Këto masa të nevojshme duhen ndërmarrë për të lehtësuar:

- Menaxhimin e ekspertizës dhe njohurive në fushën e Internetit, përshtatjen fleksibile të trajnimeve të domosdoshme në raport me kërcënimet e shpejta dhe vazhdimisht të ndryshueshme;
- Pjesëmarrjen në simulime shtetërore dhe ndërkombëtare, trajnime (punëtori, kurse etj.); Ofrimin e një programi ushtrimesh për sigurinë kibernetike për testimin dhe detajizimin e mundësive të reagimit ndaj ngjarjeve. Ushtrimet trajnuese vendore dhe ndërkombëtare luajnë rol të rëndësishëm në zhvillimin dhe vlerësimin e kapaciteteve të sigurisë kibernetike;
- Mënyrat e vetëdijesimit dhe fushatat informuese që duhen ofruar për të gjithë qytetarët e Kosovës;
- Ofrimin e kurseve adekuate për të gjitha palët e përfshira, pasi që është e rëndësishme që palët të kenë njohuri të mjaftueshme për fushën e sigurisë kibernetike. Prandaj aspektet kibernetike duhen integruar në kurrikulat ekzistuese arsimore të Kosovës.

6.2.4 Infrastruktura ligjore

Qëllimi kryesor është harmonizimi i kornizës ligjore me atë të Bashkimit Evropian. Në këtë kontest, në vitin 2016 do të hartohet për herë të parë Ligji për Identifikimin dhe Mbrojtjen e Infrastrukturës Kritike. Pjesë e rëndësishme e këtij Ligji do të jetë edhe mbrojtja e infrastrukturës kritike e informacionit.

Tutje, është identifikuar si e nevojshme që të bëhet rishikimi i Ligjit për Parandalimin dhe Luftimin e Krimit Kibernetik, si dhe të hartohen akte nënligjore të cilat mbulojnë fushën e sigurisë kibernetike.

Korniza ligjore do të ndryshohet dhe harmonizohet sipas Planit Kombëtar për Zbatimin e Marrëveshjes së Stabilizim Asociimit.

6.2.5 Kapacitetet njerëzore

Me qëllim të harmonizimit të aktiviteteve dhe trajnimeve të të gjitha institucioneve të përfshira në këtë Strategji, do të hartohen kurrikula të përbashkëta të trajnimit. Qëllimi kryesor është organizimi i trajnimeve me qëllim të përmirësimit të koordinimit dhe bashkëpunimit të institucioneve të përfshira, mirëpo do të organizohen edhe trajnime specifike për një apo grup të institucioneve.

Pjesë e rëndësishme është hartimi i skenarëve dhe mbajtja e ushtrimeve të përbashkëta, përmes së cilave institucionet e përfshira do të testojnë kapacitetet e tyre në reagim ndaj sfidave të ndryshme. Mbajtja e këtyre ushtrimeve do të përmirësoj kapacitetet në reagim ndaj kërcënimeve të ndryshme, qoftë në nivel vendi dhe institucional.

6.2.6 Infrastruktura teknike

Infrastruktura teknike luan rol të rëndësishëm në forcimin e sigurisë kibernetike në Republikën e Kosovës dhe të gjitha institucionet e përfshira janë zotuar se do të avancojnë sistemet e teknologjisë informative.

Ndër të tjera, ARKEP do të themelojë Platformën për pranimin dhe regjistrimin e incidenteve kibernetike kurse Policia e Kosovës do të avancojë pajisjet për hetimin e krimit kibernetik.

6.2.7. Hulumtimi dhe zhvillimi

Republika e Kosovës do të vazhdojë të intensifikojë hulumtimet për sigurinë e TI-së dhe për mbrojtjen e infrastrukturës kritike. Kapacitetet për Hulumtim dhe Zhvillim do të ngriten brenda Kosovës, si dhe do të shfrytëzohen edhe për pjesëmarrje në projekte shtetërore dhe ndërkombëtare, në përputhje me resurset në dispozicion.

Hulumtimi dhe zhvillimi është element kyç në përmirësimin e reagimit të Kosovës ndaj kërcënimeve të sigurisë kibernetike.

6.3 Ndërtimi i partneritetit publiko-privat (PPP)

6.3.1 Ngritja e bashkëpunimit me sektorin privat

Pasi që pjesa më e madhe e infrastrukturës kritike të informacionit i përket sektorit privat, është e domosdoshme që të definohet qartë bashkëpunimi me këtë sektor në fushën e sigurisë kibernetike.

Në veçanti, duhen përcaktuar procedurat për shkëmbimin e informatave me:

- Ofruesit e shërbimit të Internetit;
- Sektorin bankar;
- Sektorin energjetik;
- Sektorin e ujësjellësit;
- Transportin (ajror dhe tokësor);
- Fushën akademike.

Do të organizohen aktivitete të përbashkëta për edukimin mbi sigurinë kibernetike, të cilat do të fokusohen tek ofrimi i këshillave për kurrikulën e sigurisë kibernetike, certifikimin e ekspertëve të sigurisë informative dhe zhvillimin e mëtutjeshëm të moduleve mësimore.

6.4 Reagimi ndaj incidenteve

6.4.1 Funksionalizimi i CERT/CSIRT shtetërore dhe themelimi i CERT/CSIRT-ve të tjerë në Kosovë

Duke marrë parasysh që gatishmëria për siguri arrihet më së miri me alarmim dhe parandalim të hershëm, Ekipet Kompjuterike për Reagime Emergjente do të dorëzojnë raportet e tyre tek Sekretariati i Këshillit në baza të rregullta, si dhe për incidentet e veçanta. Nëse situata e sigurisë kibernetike arrin nivelin e një krize të mundshme apo që ka dodhur, Sekretariati do të informojë

drejtpërdrejt Këshillin Shtetëror për Siguri Kibernetike, të udhëhequr nga Koordinatori Nacional ose personi i autorizuar prej tij.

Sigurimi i funksionalitetit të plotë të Ekipeve Kompjuterike për Reagime Emergjente (CERT/CSIRT) brenda Kosovës është pjesë përbërëse dhe jetike e kësaj Strategjie, por edhe e përmbushjes së zotimeve të Qeverisë. Funksionet kryesore të CERT-ve/CSIRT-ve janë parandalimi i incidenteve serioze në lidhje me sigurinë e rrjeteve dhe informatave, por edhe reagimi i menjëhershëm dhe i përshtatshëm ndaj atyre incidenteve kur ato ndodhin.

Duhet theksuar që për funksionimin e mirëfilltë të një CERT-i/CSIRT-i, nevojiten:

- Infrastruktura e nevojshme, si dhe
- Personeli me trajnimet e avancuara përkatëse.

Politikat duhet të përfshijnë hapat më praktikë që një organizatë duhet të ndërmarrë kur ndodh një incident i sigurisë kibernetike. Detyrat në trajtimin e incidenteve të dokumentuara janë fillimisht të orientuara kah sigurimi i aseteve informative, –duke minimizuar dëmet sa më shpejt që është e mundur. Përtej ofrimit të mbrojtjes imediate detyrat e caktuara për përballje me incidentin do të përforcojnë të mësuarit e organizatës, si dhe mund të ndihmojnë në ndjekjen dhe hetimin e kriminelëve në fushën e sigurisë kibernetike. Është praktikë e mirë që të bëhen ushtrime për trajtimin e incidenteve, si dhe vazhdimisht të freskohen procedurat, në mënyrë që kur këto të nevojiten në situata të vërteta, të jenë të standardizuara, verifikuara dhe të besueshme.

6.4.2 Listimi dhe akreditimi i CERT-ave në Trusted Indroduced dhe First

Shpjegime të hollësishme se si të bëhet listimi në Trusted Introducer[41] dhe në FIRST[42] është në dispozicion në web-faqet e tyre. Listimi është një kërkesë e obligueshme dhe është hapi i parë për t'u bërë të akredituar dhe në këtë mënyrë duke pasur qasje edhe në shërbime vetëm për anëtarë.

6.5 Bashkëpunimi ndërkombëtar

6.5.1 Organizimi dhe pjesëmarrja në organizime ndërkombëtare

Qeveria e Kosovës do të ndjekë një qasje aktive ndaj angazhimit ndërkombëtar në sigurinë kibernetike përmes:

- nënshkrimit të marrëveshjeve dy ose shumëpalëshe me aleatët kryesorë dhe shtetet tjera për të forcuar bashkëpunimin në sigurinë kibernetike;
- pjesëmarrjes në forume rajonale, me një fokus në iniciativat për ngritjen e kapaciteteve në kuadër të rajonit;
- anëtarësimit në organizata ndërkombëtare për të ndihmuar në promovimin e praktikave më të mira ndërkombëtare dhe të zhvillojnë dhe të nxisë një qasje të koordinuar globale për luftimin e kërcënimeve të sigurisë kibernetike, duke përfshirë edhe "spam".

[41] https://www.trusted-introducer.org/processes/registration.html
[42] https://www.first.org/membership/process

6.5.2 Avancimi i bashkëpunimit ndërkombëtar

Siguria kibernetike globale mund të arrihet vetëm me mjete të koordinuara në nivel shtetëror dhe ndërkombëtar. Kosova do të luajë rol aktiv në bashkëpunimin ndërkombëtar në nivel evropian dhe global, veçanërisht me shkëmbimin e informatave, formulimin e strategjive ndërkombëtare, zhvillimin e skemave vullnetare dhe normave ligjore, ndjekjen e rasteve penale, mbajtjen e ushtrimeve ndërkombëtare, si dhe pjesëmarrjen në trajnimet dhe projektet e bashkëpunimi.

Qeveria e Republikës së Kosovës do të përkrah politikat e BE-së duke ndërmarrë masat e nevojshme për mbrojtjen e infrastrukturës kritike të informacionit, bashkëpunuar me Agjencinë Evropiane për Sigurinë e Rrjeteve dhe Informacionit (ENISA) në kuptimin e situatës së ndryshueshme të kërcënimeve në TIK, si dhe bashkëpunimin me shtetet anëtare të BE-së.

Politika e jashtme kibernetike do të përshtatet në atë mënyrë që interesat dhe synimet shtetërore për sigurinë kibernetike të koordinohen dhe të zhvillohen në harmoni me politikat e organizatave ndërkombëtare, si ENISA, OSBE, Këshilli i Evropës, OECD dhe NATO. Gjithashtu, Republika e Kosovës do të ofrojë kontributin e saj në aktivitetet anti-botnet në gjithë botën.

7 Implementimi, monitorimi dhe vlerësimi i Strategjisë

7.1 Roli i sistemit të monitorimit

Procesi i implementimit të Strategjisë do të synojë përmbushjen e objektivave strategjikë, atyre specifikë dhe aktiviteteve. Monitorimi dhe vlerësimi i rezultateve të efikasitetit të zbatimit të objektivave dhe aktiviteteve do të jetë pjesë përbërëse e Procesit të Strategjisë, si dhe elemente kyçe në përmbushjen e saj. Monitorimi dhe vlerësimi janë mjete për matjen e përparimit në raport me objektivat e caktuar, për të vlerësuar nevojën e përcaktimit të rregullave të menaxhimit, në veçanti të aktiviteteve. Procesi i monitorimit do të udhëhiqet nga Koordinatori Nacional, me pjesëmarrje të gjerë të palëve të tjera të përfshira.

Dimensionet kryesore të monitorimit dhe të vlerësimit të strategjisë janë:

- Kapaciteti institucional;
- Indikatorët e monitorimit përgjatë dhe në fund të periudhës tre vjeçare;
- Burimet e informimit dhe instrumentet e matjes.

7.2 Kapacitetet institucionale për monitorim e vlerësim

Sistemi i monitorimit dhe vlerësimit do të zgjerohet për të mbuluar të gjitha institucionet përgjegjëse për realizimin e objektivave të përcaktuara në Strategji dhe Plan të Veprimit:

- Koordinatori Nacional për Siguri Kibernetike, si institucion udhëheqës për përmbushjen e objektivave, do të monitorojë indikatorët e Strategjisë për Sigurinë Kibernetike. Në fund të çdo viti, ai do të përgatisë një raport progresi mbi objektivat;
- Ministritë dhe institucionet e tjera të shënuara në plan të veprimit do të jenë përgjegjëse për monitorimin dhe vlerësimin e aktiviteteve që u janë ndarë atyre ministrive apo institucioneve vartëse të tyre. Këto institucione do të dorëzojnë raportet e tyre periodike tek Koordinatori Nacional i Sigurisë Kibernetike, ashtu që raportet të standardizohen;.
- Organizatat joqeveritare do të marrin pjesë në procesin e monitorimit dhe vlerësimit të strategjisë, duke qenë pjesë e tryezave të rrumbullakëta që mbahen nga Koordinatori Nacional. Në këto tryeza të rrumbullakëta, organizatat joqeveritare dhe shoqëria civile do të paraqesin vlerësimet dhe rekomandimet e tyre në lidhje me gjendjen në fushën e sigurisë kibernetike.

7.3 Indikatorët për monitorim dhe vlerësim

- Numri i ligjeve dhe rregulloreve përkatëse, që kanë hyrë në fuqi pas miratimit të Strategjisë;
- Strukturat e themeluara (Koordinatori, Këshilli, Sekretariati);
- Numri i personelit të trajnuar për sigurinë kibernetike në institucionet përkatëse;
- Fushat e kurrikulës dhe librat shkollorë që trajtojnë çështjen e sigurisë kibernetike;
- Numri i projekteve dhe programeve për sigurinë kibernetike;
- Numri i raporteve të monitorimit dhe vlerësimit nga Strategjia Shtetërore për Sigurinë Kibernetike;
- Numri i aktiviteteve ndërkombëtare për sigurinë kibernetike.

7.4 Instrumentet e monitorimit dhe vlerësimit

Të dhëna administrative/statistikore nga akterët e ndryshëm të sigurisë kibernetike;
Raporti i zbatimit të Strategjisë;
Anketat për nivelin e njohurive të qytetarëve të Kosovës si rezultat i fushatave të ndërmarra të vetëdijesimit për sigurinë kibernetike.

8 Plani i Veprimit 2016-2019

Plani i Veprimit reflekton përputhshmërinë e tij me kornizën e përgjithshme të Strategjisë dhe është hartuar në kuadër të kornizës së përgjithshme strategjike të përcaktuar me Strategjinë Shtetërore për Sigurinë Kibernetike.

Plani i Veprimit do të rishikohet në fund të çdo viti në mënyrë që të sigurohet zbatueshmëria e Strategjisë dhe harmonizimi me trendet vendore dhe ndërkombëtare.

Plani i Veprimit për implementimin e kësaj strategjie përfshin:

- Objektivat strategjikë;
- Objektivat specifikë;
- Aktivitetet konkrete për implementim;
- Përcaktimin e institucioneve përgjegjëse dhe përkrahëse për përmbushjen e secilit objektiv;
- Specifikimin e kornizës kohore për përmbushjen e secilit aktivitet;
- Përcaktimin e burimeve të nevojshme financiare për zhvillimin e aktiviteteve;
- Përcaktimin e indikatorëve për implementimin e secilit objektiv dhe aktivitet.

STRATEGJIA SHTETËRORE PËR SIGURINË KIBERNETIKE PLANI I VEPRIMIT 2016 – 2019						
Objektivi Strategjik 1 Mbrojtja e Infrastrukturës Kritike të Informacionit						
Objektivi Strategjik 2 Zhvillimi institucional dhe ngritja e kapaciteteve						
2.1	**Objektivi specifik: Caktimi i Koordinatorit Nacional dhe detyrat e Këshillit Shtetëror për Sigurinë Kibernetike**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
2.1.1	Nxerrja e Vendimit të Koordinatorit Nacional për themelimin e KSHSK	K1 2016	Kosto Administrative	MPB	Institucionet relevante	Vendimi i nënshkruar
2.1.2	Organizimi i takimeve periodike (3 mujore) të KSHSK	2016-2019	Kosto e buxhetuar	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtar, (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	Numri i takimeve të mbajtura
2.1.3	Hartimi i raporteve periodike	Çdo 3 muaj	Kosto e buxhetuar	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë	Numri i raporteve të hartuara
2.1.4	Rishikimi vjetor i Planit të Veprimit	K4 2016 K4 2017 K4 2018	Donacion (OSBE)	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë (OSBE, ICITAP	Plani i Veprimit i rishikuar

					ENCYSEC, ZBE, UNDP)	
2.2	**Objektivi specifik: Ngritja e kapaciteteve në Sekretariatin e Strategjive**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
2.2.1	Përshkrimi i detyrave dhe përgjegjësive të Zyrtarit përgjegjës për zbatimin e Strategjisë të Sigurisë Kibernetike	K1 2016	Kosto Administrative	MPB	MAP, MF	Pozita e miratuar
2.2.2	Shpallja e konkursit dhe rekrutimi i zyrtarit përgjegjës	K3 2016	Kosto e buxhetuar	MPB	MAP, MF	Zyrtari i rekrutuar
2.3	**Objektivi specifik: Vetëdijesimi**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
2.3.1	Publikimi i buletinëve për situatën e sigurisë kibernetike	2016-2019 .	Kosto e buxhetuar	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	Buletinët e publikuar
2.3.2	Organizimi i fushatave vetëdijesuese	2016-2019	Donacion	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (ICITAP,	Numri i fushatave të organizuara, ligjëratat e mbajtura, fletë-palosjet e shpërndara

					ENCYSEC, ZBE, UNDP, OSBE)	
2.3.3	Plotësimi i kurrikulës aktuale të TIK-ut në nivelin para universitar me modulet e sigurisë kibernetike	2016-2017	Kosto Administrative	MASHT	Koordinatori Nacional dhe institucionet relevante	Kurrikulat e plotësuara
2.3.4	Organizimi i Muajit Evropian për Siguri Kibernetike	2016-2019	Donacion	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (ICITAP, ENCYSEC, ZBE, UNDP, OSBE	Shënimi i muajit Evropian për Sigurinë Kibernetike
2.3.5	Organizimi i seminarëve, konferencave etj.	2016-2019	Donacion (OSBE)	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (ICITAP, OSBE ENCYSEC, ZBE, UNDP)	Seminarët dhe konferencat e organizuara
2.3.6	Rritja e vetëdijes dhe bashkëpunimit me prindër, si dhe organizimi i vizitave dhe punëtorive për prindër dhe fëmijë në lidhje me rreziqet në internet	2016-2019	Kosto administrative	MASHT	MKRS, MPB, OJQ-të, partnerët ndërkombëtar dhe partnerët ndërkombëtar, (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	Punëtoritë e organizuara, vizitat në terren
2.3.7	Përfshirja e komponentës për rreziqet që vijnë nga interneti në kurrikulat e arsimit parauniversitar	2016	Kosto administrative	MASHT	DKA	Kurrikulat e plotësuara

2.3.8	Vetëdijesimi i nxënësve përmes zbatimit të kurrikulës lidhur me mbrojtjen nga rreziqet në internet	2016-2019	Kosto administrative	MASHT	MASHT, DKA, institucionet e arsimit të lartë, Inspektorati i arsimit	Kampanjat vetëdijesuese të ndërmarra
2.3.9	Përgatitja e plan-programit për ligjërim nëpër institucione shkollore lidhur me mbrojtjen e fëmijëve në internet	2016-2019	Kosto administrative	MASHT	MPB, PK, Institucionet relevante dhe partnerët ndërkombëtar (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	Plan programi, i hartuar
2.3.10	Organizimi i aktiviteteve vetëdijësuese për përdorimin e internetit të sigurt nga ana e fëmijëve	2016-2019	Kosto e buxhetuar	MASHT	MASHT, DKA, shkollat, partnerët ndërkombëtarë (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	Aktivitetet e organizuara
2.3.11	Hartimi i një udhëzimi administrativ për përdorimin e internetit në shkolla	2016-2017	Kosto e buxhetuar	MASHT	DKA, Komuniteti i prindërve, partnerët ndërkombëtarë (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	Udhëzimi administrativ i miratuar dhe shpërndarja e 12,000 manualeve
2.4	**Objektivi specifik: Infrastruktura ligjore**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
2.4.1	Rishikimi i Ligjit për Parandalimin dhe Luftimin e Krimit Kibernetik	K1 2016	Kosto Administrative	MPB	Institucionet relevante dhe partnerët ndërkombëtarë, (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	Vlerësimi i hartuar

2.4.2	Zhvillimi i Politikave dhe Procedurave Standarde të Operimit (PSO) për reagimin ndaj incidenteve kompjuterike, si dhe shpërndarja e tyre tek secila organizatë relevante që përballet me kërcënime të mëdha kibernetike	2016-2019	Kosto Administrative	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (ICITAP, ENCYSEC, ZBE, UNDP, OSBE)	PSO-të e hartuara
2.4.3	Hartimi dhe miratimi i Rregullorës për kërkesat teknike që garantojnë siguri, integritet dhe besueshmëri	K4 2016	Kosto Administrative	ARKEP	Cullen International, ekspertë të fushës	Rregullorja e miratuar nga Bordi i ARKEP
2.4.4	Hartimi dhe miratimi i Ligjit për identifikimin dhe mbrojtjen e infrastrukturës kritike	K4 2016	Kosto e buxhetuar	MPB	Institucionet relevante dhe partnerët ndërkombëtarë, (Ambasada e SHBA, ICITAP, UNDP, ENCYSEC, ZBE, OSBE)	Ligji i miratuar në Kuvend
2.5	**Objektivi specifik: Kapacitetet njerëzore**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
2.5.1	Hartimi i Kurrikulave të Trajnimit	2016-2019	Kosto e buxhetuar	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (Ambasada e SHBA, ICITAP, UNDP, ENCYSEC, ZBE, OSBE)	Numri i kurse të hartuara

2.5.2	Trajnimi dhe certifikimi i personelit të sigurisë teknologjike	2016-2019	Donacione	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (Ambasada e SHBA, ICITAP, UNDP, ENCYSEC, ZBE, OSBE)	Numri i trajnimeve dhe personelit të certifikuar
2.5.3	Hartimi i Skenarëve dhe Ushtrimeve të Sigurisë Kibernetike	2016-2019	Kosto administrative	Institucionet relevante	Partnerët ndërkombëtarë, (Ambasada e SHBA, ICITAP, UNDP, ENCYSEC, ZBE, OSBE)	Numri i skenarëve të hartuara dhe ushtrimeve të realizuara
2.6	**Objektivi specifik: Infrastruktura teknike**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
Objektivi Strategjik 3 Ndërtimi i Partneritetit Publiko-Privat (PPP).						
3.1	**Objektivi specifik: Ngritja e bashkëpunimit me sektorin privat**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
3.1.1	Caktimi i pikave të kontaktit për bashkëpunim me sektorin privat	2016	Kosto Administrative	Koordinatori Nacional	Sektori Privat	Pikat e kontaktit të sektorit privat të caktuara
3.1.2	Bashkëpunimi me ofruesit e shërbimeve të internetit dhe komunikimit për identifikim dhe mbrojtje nga aktivitet e dëmshme	2016-2019	Kosto Administrative	Koordinatori Nacional	Sektori Privat	Numri i shkëmbimi të informatave

3.1.3	Krijimi, në bashkëpunimin me sektorin privat, i kritereve minimale të detyrueshme për mbrojtje të infrastrukturës kritike të informacionit	2016	Kosto Administrative	Koordinatori Nacional	Sektori Privat	Kriteret minimale të detyrueshme të hartuara
3.1.4	Organizimi i takimeve të rregullta në mes sektorit publik dhe privat	2016-2019	Kosto e buxhetuar	Koordinatori Nacional	Sektori Privat	Numri i takimeve të mbajtura
Objektivi Strategjik 4 Reagimi ndaj incidenteve						
Objektivi Strategjik 5 Bashkëpunimi ndërkombëtar						
5.1	**Objektivi specifik: Organizimi dhe pjesëmarrja në organizime ndërkombëtare**					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
5.1.1	Organizimi i aktiviteteve ndërkombëtare të sigurisë kibernetike dhe ngjarjeve vjetore	2016-2019	Donacion	Koordinatori Nacional	Institucionet relevante dhe partnerët ndërkombëtarë, (ICITAP, OSBE, ENCYSEC, ZBE, UNDP)	Numri i aktiviteteve të organizuara
5.1.2	Pjesëmarrja në aktivitetet ndërkombëtare në fushën e sigurisë kibernetike	2016-2019	Donacion	Institucionet relevante	Koordinatori Nacional, partnerët ndërkombëtarë (ICITAP, OSBE, ENCYSEC, ZBE, UNDP)	Numri i aktiviteteve dhe numri pjesëmarrësve

5.2	Objektivi specifik: Avancimi i bashkëpunimit ndërkombëtar					
Nr.	**Aktiviteti**	**Afati kohor**	**Buxheti**	**Institucioni përgjegjës**	**Institucionet mbështetëse**	**Indikatorët e performancës**
5.2.1	Vendosja e partneritetit me ENISA	2016-2019	Kosto e buxhetuar	Koordinatori Nacional	MPB,MFSK, PK, ARKEP, ASHI,	Numri i vizitave, pjesëmarrjeve, ushtrimeve dhe aktiviteteve tjera të organizuara nga ENISA
5.2.2	Avancimi i bashkëpunimit rajonal dhe ndërkombëtar në luftën kundër krimit kibernetik	2016-2019	Kosto Administrative	PK, AKI,DK, NJIF, KPK, KGJK	Institucionet relevante	Numri i informatave të shkëmbyera, numri i hetimeve të përbashkëta, numri i operacioneve të përbashkëta
5.2.3	Themelimi i Pikës së Përhershme të kontaktit 24/7 për bashkëpunim ndërkombëtar në fushën e krimit kibernetik	2016	Kosto e buxhetuar	Koordinatori Nacional, MPB, PK	Institucionet relevante	Pika e kontaktit 24/7 e themeluar