REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. ____ Prot. Tiranë më, ____ .____. 2024

RAPORT MONITORIMI

I

STRATEGJISË KOMBËTARE

PËR SIGURINË KIBERNETIKE 2020-2025

VITI 2023

DREJTOR I PËRGJITHSHËM

Igli Tafa

Tiranë, 2024

TABELA E PËRMBAJTJES

1. HYRJE 2

2. METODOLOGJIA E MONITORIMIT 4

3. POLITIKAT E STRATEGJISË 5

3.1 QËLLIMI I POLITIKËS 1. GARANTIMI I SIGURISË KIBERNETIKE NË NIVEL KOMBËTAR, NËPËRMJET MBROJTJES SË INFRASTRUKTURAVE TË INFORMACIONIT, DUKE FUQIZUAR MJETET TEKNOLOGJIKE DHE JURIDIKE 5

3.1.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK) 5

3.1.2 POLICIA E SHTETIT (PSH) 12

3.1.3 AGJENCIA KOMBËTARE E SHOQËRISË SË INFORMACIONIT (AKSHI) 13

3.2 QËLLIMI I POLITIKËS 2. NDËRTIMI I NJË MJEDISI TË SIGURT KIBERNETIK DUKE EDUKUAR DHE NDËRGJEGJËSUAR SHOQËRINË NË NGRITJEN E KAPACITETEVE PROFESIONALE NË FUSHËN E SIGURISË SË INFORMACIONIT. 15

3.2.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK) 16

3.3 QËLLIMI I POLITIKËS 3. KRIJIMI I MEKANIZMAVE TË NEVOJSHËM PËR SIGURINË E FËMIJËVE NË HAPËSIRËN KIBERNETIKE, DUKE PËRGATITUR NJËKOHËSISHT BREZIN E RI TË AFTË PËR TË PËRFITUAR NGA PËRPARËSITË E TEKNOLOGJISË SË INFORMACIONIT DHE PËR TË PËRBALLUAR SFIDAT E ZHVILLIMIT 19

3.3.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK) 19

3.3.2 MINISTRIA E ARSIMIT DHE SPORTIT (MAS) 21

3.3.3 POLICIA E SHTETIT (PSH) 24

3.3.4 MINISTRIA E SHËNDETËSISË DHE MBROJTJES SOCIALE (MSHMS) 25

3.4 QËLLIMI I POLITIKËS 4. RRITJA E BASHKËPUNIMIT KOMBËTAR DHE NDËRKOMBËTAR NË FUSHËN E SIGURISË KIBERNETIKE ME PARTNERËT STRATEGJIKË 27

3.4.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK) 27

4. REKOMANDIME 31

1. HYRJE

Siguria kibernetike në Republikën e Shqipërisë ka marrë një rëndësi të veçantë brenda agjendës së sigurisë kombëtare gjatë viteve të fundit, duke u pasqyruar qartë në angazhimet e qeverisë për të adresuar dhe përballuar sfidat e sigurisë kibernetike. Në kontekstin e mjedisit strategjik ndërkombëtar dhe kombëtar, një digjitalizim i shpejtë i shërbimeve dhe jo vetëm, si dhe sulmet kibernetike në rritje që targetuan infrastrukturat kritike dhe të rëndësishme të informacionit, gjatë vitit 2023, qeveria shqiptare ka punuar me angazhim maksimal për forcimin e sigurisë kibernetike, në një linjë me Strategjinë Kombëtare për Sigurinë Kibernetike 2020-2025. Duke konsideruar kërcënimet në rritje dhe nevojat për të garantuar një ekosistem të sigurt dhe të qëndrueshëm kibernetik, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike është angazhuar për rishikimin e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike për periudhën 2024-2025. Në këtë kuadër është hartuar një plan i ri strategjik, në konsultim me të gjithë aktorët e përfshirë, që parashikon masa për modernizimin e politikave të sigurisë kibernetike dhe infrastrukturës teknologjike në përputhje me standardet ndërkombëtare, rritjen e ndërgjegjësimit dhe sigurisë *online* për qytetarët dhe me fokus të veçantë fëmijët dhe të rinjtë, si dhe forcimin e bashkëpunimit kombëtar dhe ndërkombëtar.

Në kuadër të punës për përmirësimin e kornizës politike dhe ligjore si dhe procesit të përafrimit të legjislacionit me *acquis* e Bashkimit Evropian, qeveria shqiptare ka punuar për hartimin e një ligji të ri që rregullon fushën e sigurisë kibernetike duke transpozuar Direktivën (BE) Nr. 2022/2555 (NIS 2).

Gjithashtu, një progres i rëndësishëm është bërë në forcimin e kapaciteteve teknologjike dhe profesionale të Qendrës Kombëtare Operacionale të Sigurisë Kibernetike (SOC Kombëtar) si dhe Ekipit të Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike pranë Autoritetit (CSIRT Kombëtar), me qëllim garantimin e sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit.

Po ashtu, edukimi dhe ndërgjegjësimi i shoqërisë, si dhe rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit në sektorin publik dhe privat kanë qenë në fokus të punës së AKCESK gjatë vitit 2023, me qëllim krijimin e një kulture të sigurisë kibernetike në shoqëri si dhe përgatitjen e një brezi profesionistësh të aftë për të adresuar sfidat e sigurisë kibernetike. Një progres i rëndësishëm është shënuar në kuadër të forcimit të bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike me partnerët strategjikë, ku janë nënshkruar një sërë marrëveshjesh bashkëpunimi, si dhe vijon puna për ta zgjeruar këtë bashkëpunim.

Në këtë kontekst, raporti i monitorimit për vitin 2023 ofron një pasqyrë të hollësishme të progresit të arritur në realizimin e objektivave strategjikë të sigurisë kibernetike. Raporti dokumenton realizimin e aktiviteteve të planifikuara, vlerëson efikasitetin e masave të marra dhe identifikon fushat ku nevojiten përpjekje të mëtejshme. Me një fokus të qartë në sigurinë dhe qëndrueshmërinë kibernetike afatgjatë, qeveria shqiptare është e angazhuar të vazhdojë punën e saj për të qenë një model në rajonin e Ballkanit dhe më gjerë për menaxhimin e sfidave

në fushën e sigurisë kibernetike, duke kontribuar kështu për një hapësirë kibernetike më të sigurt edhe në nivel global.

Raporti i Monitorimit është hartuar duke shqyrtuar nivelin e realizimit të të gjitha masave të parashikuara në Strategjinë Kombëtare për Sigurinë Kibernetike. Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025, miratuar me Vendimin nr. 1034, datë 24.12.2020, të Këshillit të Ministrave, përbën një instrument kyç për rritjen e sigurisë së rrjeteve dhe sistemeve të informacionit në nivel kombëtar, duke e konsideruar sigurinë kibernetike prioritet të qeverisë shqiptare.

Kjo strategji synon garantimin e sigurisë kibernetike në Republikën e Shqipërisë nëpërmjet, ngritjes dhe funksionimit të mekanizmave bashkëveprues institucional, instrumenteve ligjore dhe teknike, si elemente thelbësore të mbrojtjes në hapësirën kibernetike për infrastrukturat e informacionit, transaksionet dhe komunikimet elektronike; nëpërmjet ngritjes së kapaciteteve profesionale, rritjes së vetëdijes mbarëkombëtare, si dhe forcimit të bashkëpunimeve kombëtare dhe ndërkombëtare për një mjedis digjital të sigurt.

Strategjia mbështetet në parimet themelore të mëposhtme:

- zbatimi i vlerave të njëjta themelore në botën fizike dhe digjitale;
- mbrojtja e të drejtave themelore, liria e shprehjes, të dhënat personale dhe privatësia;
- qasja për të gjithë;
- qeverisje demokratike dhe efikase;
- përgjegjësi e përbashkët në garantimin e sigurisë kibernetike.

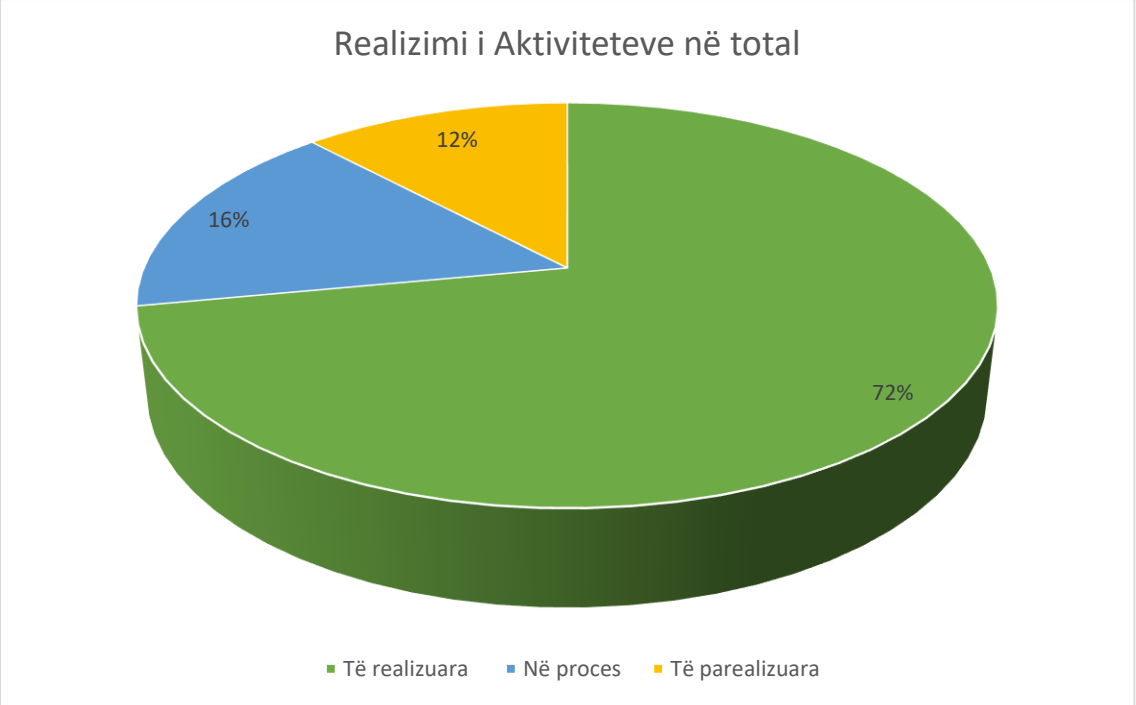
Aktorët e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 janë:

- Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike;
- Policia e Shtetit;
- Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar;
- Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm;
- Agjencia Kombëtare e Shoqërisë së Informacionit;
- Ministria e Shëndetësisë dhe Mbrojtjes Sociale;
- Ministria e Arsimit dhe Sportit.

Realizimi i aktiviteteve të Planit të Veprimit[1]

Sa i përket zbatimit të Planit të Veprimit, rezulton se deri në vitin 2023, shkalla e realizimit të aktiviteteve në % është: aktivitete të realizuara 72% (90 aktivitete), aktivitete në proces 16% (20 aktivitete) dhe aktivitete të parealizuara 12% (15 aktivitete). Bazuar tek këto të dhëna, arrihet në përfundimin se sa i përket rezultateve të arritura dhe aktiviteteve të zbatuara më shumë progres ka pasur në realizimin e Qëllimit të Politikës 1 dhe Qëllimit të Politikës 3.

[1] ***Shënim:*** *Monitorimi i realizimit të aktiviteteve të Planit të Veprimit për vitin 2023 është mbyllur në Maj 2024 dhe është vijuar me hartimin e raportit. Për aktivitetet që gjatë vitit 2023 kanë qenë në proces dhe janë realizuar në vitin 2024 përpara mbylljes së monitorimit, është dhënë informacioni për realizimin tyre, por nuk janë llogaritur si aktivitete të realizuara gjatë 2023 në këtë raport.*



2. METODOLOGJIA E MONITORIMIT

Vlerësimi i realizimit të objektivave të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, do të bëhet duke ndjekur në mënyrë periodike realizimin e planit të aktiviteteve të parashikuara për periudhën si dhe ecurinë e indikatorëve kryesorë të monitorimit.

Analiza e këtij raporti është mbështetur kryesisht në monitorimin e realizimit të aktiviteteve të parashikuara në planin e veprimit që përfshin periudhën Janar – Dhjetor 2023.

Monitorimi i Strategjisë ka konsistuar në këto faza kryesore:

a) Raportimi i institucioneve mbi zbatimin e masave për arritjen e rezultateve për të cilat janë përgjegjëse; dhe

b) Monitorimi i indikatorëve të matshëm për Strategjinë Kombëtare për Sigurinë Kibernetike.

Me qëllim realizimin e sa më sipër, janë ndjekur hapat si më poshtë vijojnë:

- Është kryer paraprakisht analiza e aktiviteteve të planit të veprimit sipas çdo objektivi strategjik;

- Janë identifikuar institucionet përgjegjëse për zbatimin e tyre;

- Është komunikuar me shkresë me çdo institucion dhe koordinuar në vazhdimësi me pikat e kontaktit për raportimin e statusit të realizimit sipas metodologjisë.

3. POLITIKAT E STRATEGJISË

3.1 QËLLIMI I POLITIKËS 1. GARANTIMI I SIGURISË KIBERNETIKE NË NIVEL KOMBËTAR, NËPËRMJET MBROJTJES SË INFRASTRUKTURAVE TË INFORMACIONIT, DUKE FUQIZUAR MJETET TEKNOLOGJIKE DHE JURIDIKE.

Objektivat e prioritetit fokusohen në:

- Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i tij me direktivat dhe rregulloret e Bashkimit Evropian;
- Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar;
- Fuqizimi dhe implementimi i masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit;
- Përmirësimi i infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizimin dhe ekstremizmin e dhunshëm.

Për realizimin e ***objektivave të prioritetit të parë strategjik***, institucionet e përfshira në realizimin e Planit të Veprimit, bazuar në raportimet e tyre, kanë arritur rezultatet si më poshtë vijon:

3.1.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK)

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) ka punuar për analizën e legjislacionit të sigurisë kibernetike dhe hendekut ligjor dhe institucional për direktivat dhe rregulloret e BE-së që normojnë fushën e sigurisë kibernetike. Në kuadër të procesit të shqyrtimit analitik (*screening*) si një nga fazat e procesit të integrimit evropian, AKCESK ka analizuar *acquis* e Bashkimit Evropian në fushën e sigurisë kibernetike për kapitujt 10, 20, 31, dhe 24, si dhe ka bërë krahasimet me legjislacionin shqiptar, duke identifikuar aktet e BE-së që duhen implementuar. Gjithashtu, në kuadër të këtij procesi, AKCESK ka analizuar kapacitetet institucionale dhe administrative për të vlerësuar nivelin aktual si dhe nevojat për rritje kapacitetesh në vijim. Pas kësaj analize, AKCESK ka kontribuar në përgatitjen e prezantimeve, për kapitujt e *acquis* ku është pjesë e grupeve ndërinstitucionale të punës, të cilat janë mbajtur në takime bilaterale me Komisionin Evropian, duke paraqitur situatën aktuale dhe angazhimet e ardhshme në këtë fushë.

Me qëllim përafrimin e kuadrit ligjor në fuqi në fushën e identifikimit elektronik, shërbimeve të besuara dhe sigurisë kibernetike me legjislacionin e BE-së, Autoriteti ka punuar me procesin e përafrimit të *acquis* si vijon:

- Rregullorja e BE, nr.910/2014 eIDAS, për përafrimin e plotë të projektligjit "Për identifikimin elektronik dhe shërbimet e besuara me këtë rregullore;

- Direktiva NIS1 me qëllim përafrimin me këtë direktivë të projektligjit "Për sigurinë kibernetike", ku Autoriteti fillimisht hartoi një draft-ligj duke e përafruar plotësisht me këtë Direktivë.

Me hyrjen në fuqi të Direktivës NIS2 në dhjetor të vitit 2022 (*Direktiva nr.2022/2555 të Parlamentit dhe Këshillit Evropian, datë 14 dhjetor 2022 "Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, duke ndryshuar Rregulloren (BE) nr.910/2014 dhe Direktivën (BE) nr. 2018/1972, dhe duke shfuqizuar Direktivën (BE) nr. 2016/1148*), duke marrë në konsideratë risitë e sjella nga kjo e fundit dhe duke qenë se kjo Direktivë shfuqizonte Direktivën NIS 1, Autoriteti filloi procesin e studimit dhe përafrimit të kësaj direktive.

Me përfundimin e draftit fillestar, në përputhje me ligjin nr. 146/2014, "Për njoftimin dhe konsultimin publik", projektligji "Për sigurinë kibernetike" u publikua në Regjistrin Elektronik për Njoftimet dhe Konsultimet Publike (RENJKP) nga data 26 prill 2023 deri më 24 maj 2023. Autoriteti zhvilloi seanca konsultimi me palët e interesuara, duke përfshirë edhe subjektet e infrastrukturës kritike dhe të rëndësishme të informacionit, që u ftuan të merrnin pjesë dhe të jepnin kontribut përmes komenteve dhe sugjerimeve.

Pas përfundimit të fazës së konsultimit publik dhe marrjes së komenteve dhe sugjerimeve, Autoriteti vazhdoi punën e tij për transpozimin gjithëpërfshirës të dispozitave të Direktivës (BE) Nr. 2022/2555 (NIS 2). Ky proces përfshinte edhe vlerësimin dhe reflektimin e komenteve përkatëse të marra nga institucionet, grupet e interesit, si dhe përgatitjen e paketës së plotë të projektligjit.

Për vitin 2023 u përmbyll procesi i hartimit të draftit final të ligjit "Për sigurinë kibernetike" dhe paketës shoqëruese te tij, i cili në dhjetor të këtij viti u dërgua në Kryeministri për vijimin me procedurat e mëtejshme.

Projektligji kaloi më pas në procedurat e nevojshme për miratim në Kuvendin e Republikës së Shqipërisë. Ligji i ri 25/2024 "Për Sigurinë Kibernetike" hyri në fuqi më datë 3 maj 2024. Niveli i transpozimit të direktivës NIS2 konsiston në një nivel të lartë të përputhshmërisë me Direktivën NIS 2.

Lidhur me projektligjin " Për identifikimin elektronik dhe shërbimet e besuara" në maj të vitit 2023 u përmbyll drafti final i ligjit dhe paketa shoqëruese e tij, i përafruar plotësisht me rregulloren e BE nr.910/2014, eIDAS, i cili është dërguar në Kryeministri për vijimin me procedurat e mëtejshme. Për shkak të riinxhinierimit të shërbimeve, projektligji u rikthye për t'u rishikuar në tërësinë e tij.

Përgjatë vitit 2023 nga ana e Autoritetit janë studiuar praktikat më të mira të shteteve të zhvilluara lidhur me përcaktimin e procedurës kombëtare për rastet e gjendjeve të

jashtëzakonshme të krijuar nga krizat kibernetike, me qëllim përpunimin dhe përzgjedhjen e modelit më të mirë të përcaktimit të kësaj procedure në zbatim të akteve nënligjore të projektligjit për sigurinë kibernetike.

Duke marrë parasysh kërcënimet në rritje të sigurisë kibernetike dhe sulmet ndaj infrastrukturave kritike të informacionit të Shqipërisë, qeveria shqiptare ka shtuar përpjekjet e saj për të arritur një nivel të lartë sigurie kibernetike në nivel kombëtar. Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025 parashikon nevojën e rishikimit të Planit të Veprimit përkatës çdo dy vjet, bazuar në dinamikën e zhvillimit të sektorit të sigurisë kibernetike.

Në këtë kuadër, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) ka rishikuar Planin e Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike për periudhën 2024-2025, duke hartuar një plan të ri strategjik në përputhje me qëllimet e politikës dhe objektivat specifike të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025. Ky plan veprimi, përveç AKCESK, përfshin gjithashtu edhe disa institucione të tjera, si Policia e Shtetit, Agjencia Kombëtare e Shoqërisë së Informacionit, Ministria e Arsimit dhe Sportit, Ministria e Shëndetësisë dhe Mbrojtjes Sociale, Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar, Ministria e Infrastrukturës dhe Energjisë, Autoriteti i Komunikimeve Elektronike dhe Postare, Qendra e Koordinimit kundër Ekstremizmit të Dhunshëm, Agjencia Shtetërore për Mbrojtjen e të Drejtave të Fëmijëve dhe Ministria për Evropën dhe Punët e Jashtme, të cilat do të jenë përgjegjëse për zbatimin e tij.

Procesi i rishikimit ka përfshirë koordinim dhe konsultime periodike me të gjitha institucionet përgjegjëse dhe grupet e interesit në lidhje me draftin paraprak të planit të ri të veprimit të hartuar, përmes takimeve dhe komunikimeve të vazhdueshme me email për të kërkuar mendim dhe sugjerime, si dhe integruar komentet përkatëse të të gjitha palëve të përfshira në përputhje me objektivat strategjikë. Pas integrimit të komenteve dhe sugjerimeve të palëve të përfshira, Plani i Veprimit 2024-2025 është konsultuar edhe me ekspertët e Shkollës Rajonale të Administratës Publike për të kryer një parashikim dhe analizë sa më të saktë sa i përket buxhetit të nevojshëm, duke çuar në përgatitjen e versionit përfundimtar të këtij plani.

Plani i Veprimit 2024-2025 i Strategjisë Kombëtare për Sigurinë Kibernetike është një plan strategjik ambicioz dhe zbatimi i tij do të kontribuojë në përpjekjet e qeverisë për të garantuar sigurinë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit, rritjes së kapaciteteve dhe ndërgjegjësimit, krijimit të mekanizmave të nevojshëm për sigurinë e qytetarëve në hapësirën kibernetike, me fokus fëmijët dhe të rinjtë, dhe rritjes së bashkëpunimit kombëtar dhe ndërkombëtar me partnerët strategjikë në fushën e sigurisë kibernetike.

Ky plan i ri veprimi adreson prioritetet, nevojat dhe sfidat sa i përket sigurisë kibernetike në nivel kombëtar, nëpërmjet parashikimit të aktiviteteve të nevojshme në përputhje me qëllimet dhe objektivat specifike përkatëse. Këto aktivitete synojnë përmirësimin e politikave dhe procedurave, rritjen e kapaciteteve teknike dhe njerëzore, forcimin e strukturave dhe infrastrukturave të sigurisë kibernetike, parandalimin dhe reduktimin e fenomeneve si krimi kibernetik dhe përmbajtjet e paligjshme në internet që kërcënojnë sigurinë e qytetarëve në hapësirën kibernetike, si dhe forcimin e bashkëpunimit kombëtar dhe ndërkombëtar, duke

synuar rritjen e përgatitjes dhe qëndrueshmërisë së Shqipërisë në fushën e sigurisë kibernetike. Plani i Veprimit 2024-2025 do të kontribuojë për të arritur rezultatet e mëposhtme të synuara edhe nga Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025:

- Përmirësimi i kornizës politike dhe ligjore, duke përfshirë ligjet, politikat strategjike, rregulloret, metodologjitë dhe procedurat, përmes implementimit të politikave dhe standardeve të sigurisë kibernetike të BE-së gjithashtu;

- Fuqizimi i strukturave dhe infrastrukturave të sigurisë kibernetike sa i përket kapaciteteve teknike dhe profesionale si dhe procedurave e tyre përkatëse. Kjo planifikohet të arrihet përmes aktiviteteve të tilla si: përmirësimi i kapaciteteve të Qendrës Kombëtare Operacionale të Sigurisë Kibernetike (SOC) për monitorimin dhe trajtimin e incidenteve të sigurisë kibernetike, ngritja e laboratorëve të analizave të programeve me qëllim të keq (*malware*) dhe simulimit të incidenteve kibernetike, rritja e kapaciteteve teknike dhe profesionale, analiza teknologjike të mjedisit të infrastrukturave kritike, optimizimi i infrastrukturës së sigurisë, përmirësimi i procedurave të trajtimit dhe menaxhimit të incidenteve dhe të tjera, të cilat parashikohen në planin e veprimit;

- Rritja e ndërgjegjësimit dhe edukimi, si dhe përmirësimi i masave parandaluese dhe mbrojtëse në lidhje me kërcënimet e sigurisë kibernetike, krimin kibernetik dhe përmbajtjet e paligjshme në internet, sigurinë në internet dhe mbrojtjen e fëmijëve në internet, si dhe ekstremizmin e dhunshëm dhe radikalizimin në hapësirën kibernetike;

- Rritja e kapaciteteve profesionale në siguri kibernetike përmes programeve arsimore. Për të arritur këtë, plani i veprimit i rishikuar parashikon hartimin e programeve të reja të studimit dhe përditësimin e kurrikulave ekzistuese të arsimit të lartë në fushën e sigurisë kibernetike, mundësimin e kurseve *online*, programe trajnimi dhe stërvitje kibernetike për ekspertët e sigurisë kibernetike të institucioneve, operatorëve të infrastrukturave kritike të informacionit (OIKI) dhe operatorëve të infrastrukturave të rëndësishme të informacionit (OIRI);

- Forcimi i bashkëpunimit kombëtar dhe ndërkombëtar, ku janë planifikuar disa aktivitete, të tilla si: krijimi i një forumi me institucione publike dhe private në Shqipëri dhe agjenci ndërkombëtare, krijimi i një strukture të diplomacisë kibernetike në Ministrinë për Evropën dhe Punët e Jashtme në koordinim me AKCESK, hartimi dhe nënshkrimi i marrëveshjeve dypalëshe dhe shumëpalëshe në fushën e sigurisë kibernetike, promovimi dhe zbatimi i ligjit ndërkombëtar, normave dhe masave të ndërtimit të besimit në lidhje me sjelljen e përgjegjshme të shtetit në hapësirën kibernetike, pjesëmarrje aktive në OKB, NATO, OSBE, BE dhe organizata të tjera ndërkombëtare, stërvitje rajonale kibernetike, pjesëmarrje në projekte ndërkombëtare, etj.

Plani i Veprimit 2024-2025 kontribuon gjithashtu në procesin e integrimit evropian të Shqipërisë, pasi parashikon aktivitete në lidhje me përmirësimin e kuadrit ligjor dhe të politikave aktuale nëpërmjet zbatimit të politikave të BE-së, standardeve të sigurisë kibernetike dhe praktikave më të mira, si dhe bashkëpunimit ndërkombëtar me partnerët strategjikë.

Duke konsideruar Strategjinë Kombëtare për Sigurinë Kibernetike, ngritja dhe fuqizimi i CSIRT-it Kombëtar ka qenë dhe mbetet prioritet kyç. Që nga fillimi i kësaj nisme, janë

ndërmarrë hapa të rëndësishëm për të siguruar që CSIRT-i Kombëtar të jetë i pajisur me procedurat dhe kapacitetet e nevojshme teknike dhe njerëzore për të përballuar sfidat kibernetike.

Gjatë vitit 2023, është hartuar dhe miratuar procedura për menaxhimin e incidenteve (v 1.0), e cila përmban masa të detajuara për identifikimin, vlerësimin, dhe menaxhimin efektiv të incidenteve kibernetike. Kjo procedurë siguron një qasje të strukturuar dhe të koordinuar për të minimizuar ndikimin e incidenteve në sistemet dhe të dhënat kritike, duke kontribuar në forcimin e sigurisë kibernetike në nivel kombëtar.

Me qëllim rritjen e kapaciteteve të Ekipit të Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike pranë Autoritetit (CSIRT Kombëtar) është realizuar modernizimi i infrastrukturës teknologjike, duke siguruar që CSIRT-i të jetë i pajisur me mjetet dhe teknologjitë më të avancuara për të detektuar, parandaluar dhe luftuar kërcënimet kibernetike.

Për të përforcuar më tej kapacitetet e CSIRT-it Kombëtar, AKCESK ka punuar për plotësimin e strukturës së planifikuar me staf të ri ku procesi i rekrutimit vijon. Në këtë kuadër, prioritet i Autoritetit ka qenë tërheqja e talenteve dhe profesionistëve në fushën e sigurisë kibernetike, të cilët do të kontribuojnë në zhvillimin e strategjive parandaluese dhe forcimin e përgjigjes ndaj incidenteve.

AKCESK, në përmbushje të detyrave, ka punuar për sigurimin e një mjedisi pune funksional dhe efikas për Qendrën Kombëtare Operacionale të Sigurisë Kibernetike (SOC Kombëtar) për të garantuar sigurinë kibernetike në infrastrukturat kritike e të rëndësishme të informacionit.
SOC Kombëtar ka bërë hapa të rëndësishëm në përballjen e sfidave të sigurisë kibernetike. Qendra SOC luan një rol kyç në monitorimin, analizimin dhe reagimin ndaj incidenteve kibernetike në infrastrukturat kritike të informacionit. Në këtë proces, aspekt kyç ka qenë krijimi i kushteve optimale të punës, që përfshijnë zhvillimin e infrastrukturës teknike, rritjen e kapaciteteve njerëzore, dhe forcimin e bashkëpunimit strategjik.

Në terma të zhvillimit të infrastrukturës, SOC Kombëtar ka kaluar në një transformim të rëndësishëm, duke përfshirë implementimin e mjeteve të avancuara të monitorimit dhe analizës së sigurisë, të cilat mundësojnë identifikimin dhe menaxhimin proaktiv të kërcënimeve kibernetike. Përmes partneriteteve strategjike dhe investimeve janë siguruar teknologji dhe mjete që përshtaten me nevojat specifike të infrastrukturave të informacionit.

Një element kyç ka qenë fuqizimi i kapaciteteve njerëzore përmes programeve të vazhdueshme të trajnimit dhe zhvillimit profesional. Punonjësit e SOC kanë marrë pjesë në sesione trajnimi dhe workshope, të fokusuara jo vetëm në aspektet teknike, por edhe në menaxhimin e krizave dhe komunikimin efektiv gjatë incidenteve. Përveç kësaj, është krijuar një program mentorimi për të ndihmuar në zhvillimin e shpejtë të aftësive të stafit të ri.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka punuar gjithashtu edhe për rritjen e kapaciteteve të CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar nëpërmjet trajnimeve dhe stërvitjeve kibernetike duke tejkaluar objektivin e vendosur që synonte minimumi 4 stërvitje dhe ushtrime kibernetike në vit. Gjatë vitit 2023 janë organizuar

rreth 12 stërvitje kibernetike. Ky rezultat reflekton përkushtimin e AKCESK në përmirësimin dhe forcimin e sigurisë kibernetike në nivel kombëtar.

Gjatë vitit 2023 është bërë progres sa i përket fuqizimit dhe implementimit të masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe analizimit të infrastrukturave kritike dhe të rëndësishme të informacionit për vlerësimin e menaxhimin e riskut në to.

Në përmbushje të detyrave funksionale si dhe në zbatim të ligjit nr. 2/2017, "Për Sigurinë Kibernetike", Vendimit të Këshillit të Ministrave nr. 553, datë 15.07.2020, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", i ndryshuar, dhe rregullores "Mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë"*(V. 2.0, miratuar me Urdhrin Nr. 10/2022)*, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike gjatë periudhës janar- dhjetor 2023, ka kryer kontrolle fizike të vazhdueshme të sigurisë kibernetike në ambjentet e operatorëve *(onsite)* pranë infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me implementimin e masave minimale të sigurisë. Si rezultat i një pune intensive, përgjatë vitit 2023 u katërfishua numri i kontrolleve me vajtje në vend në infrastrukturat kritike dhe të rëndësishme të informacionit.

Bazuar në situatën aktuale të sigurisë kibernetike si dhe emergjencës për të rritur nivelin e sigurisë në infrastrukturat e informacionit u hartuan masa teknike shtesë (*Baseline*), miratuar si pjesë integrale e "Rregullores mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë". Baseline përmban 28 masa minimale teknike të sigurisë kibernetike të detyrueshme për t'u implementuar nga OIRI dhe OIKI.

AKCESK ka organizuar gjithashtu takime konsultuese me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit mbi rëndësinë e implementimit të masave teknike shtesë të sigurisë kibernetike (*Baseline*) brenda afateve të përcaktuara. AKCESK ka realizuar vlerësimin e implementimit të këtyre masave në nivel infrastrukture si dhe në nivel sektorial.

Konkretisht, gjatë vitit 2023, AKCESK ka kontrolluar për zbatimin e masave të sigurisë kibernetike:

- 26 Operatorë të Infrastrukturave Kritike të Informacionit, në sektorët Shëndetësor, Financiar (Bankar, Mikrofinanciar) dhe Energjetik (me metodën vajtje ne vend);
- 32 operatorë të Infrastrukturave Kritike të Informacionit (me metodën vetëdeklarim);
- 23 Operatorë të Infrastrukturave të Rëndësishme të Informacionit, në sektorët Energjetik, Transportin, Shëndetësor dhe Financiar (Tregu i Siguracioneve), Furnizimi me ujë (me metodën vajtje në vend);
- 22 operatorë të infrastrukturave të rëndësishme të informacionit (me metodën vetëdeklarim).

Vlerësimi i masave teknike të sigurisë u bazua në masat emergjente, si dhe në Programin e Ri për vlerësimin e dobësive të sigurisë kibernetike *GAP Analysis*.

Gjithashtu nëpërmjet metodës së vetëdeklarimit, përgjatë vitit 2023 është realizuar vlerësimi i implementimit të masave të sigurisë kibernetike për institucionet e sigurisë dhe mbrojtjes, të cilat nuk janë pjesë e infrastrukturave kritike dhe të rëndësishme te informacionit, përkatësisht për:

1. Ministrinë e Mbrojtjes;
2. Drejtorinë e Përgjithshme të Policisë së Shtetit;
3. Agjencinë e Mbikëqyrjes Policore;
4. Drejtorinë e Sigurimit të Informacionit të Klasifikuar;
5. Këshillin e Lartë Gjyqësor;
6. Këshillin e Lartë të Prokurorisë;
7. Kuvendin;
8. Institucionin e Presidentit të Republikës;
9. Inspektoratin e Lartë të Deklarimit dhe Kontrollit të Pasurive dhe Konfliktit të Interesave;
10. Prokurorinë e Përgjithshme;
11. Komisionin Qendror të Zgjedhjeve.

Me qëllim automatizimin e procesit të kontrollit të nivelit të implementimin të masave të sigurisë, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka implementuar CISA CSET TOOL. Kjo platformë shërbeu për digjitalizimin e procesit të kontrollit si dhe për krijimin e një databaze elektronike për kontrollet e kryera, nivelin e implementimit te masave si dhe nivelin e sigurisë për çdo institucion të vlerësuar.

Disa nga funksionalitetet kryesore te CSET TOOL përfshijnë:

- Kontrollin efektiv të implementimit të masave të sigurisë nga OIKI dhe OIRI;
- Analizimin e dobësive të sigurisë kibernetike të OIKI dhe OIRI;
- Vlerësimin e nivelit të sigurisë kibernetike (*Cyber Resilience*), si dhe vlerësimin e riskut të OIKI dhe OIRI;
- Krijimin e profileve të dedikuara për të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit, sipas sektorëve specifikë;
- Gjenerimin e raporteve (në mënyrë statistikore/grafike) për nivelin e sigurisë kibernetike të infrastrukturave;
- Rekomandime për përmirësimin e dobësive të evidentuara gjatë kontrolleve.

Me qëllim garantimin e mirëqeverisjes së sigurisë kibernetike në nivel kombëtar, investimet në siguri kibernetike në sektorin publik dhe privat kanë një rol thelbësor. Për të pasur një pasqyrë të situatës së investimeve në siguri kibernetike, në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, u realizua analiza mbi buxhetet e

dedikuara për sigurinë kibernetike për vitin 2023 dhe vitin 2024, si dhe investimet në sigurinë kibernetike për vitin 2023.

Gjatë vitit 2023, AKCESK ka hartuar edhe udhëzimin "*Udhëzimi për metodologjinë e përcaktimit të dënimeve administrative në procesin e kontrollit të infrastrukturave kritike dhe të rëndësishme të informacionit*", miratuar nga Drejtori i Përgjithshëm me Nr.179 Prot., datë 03.03.2023.

Pas kryerjes së procesit të kontrollit "Mbi evadimin e zbatimit të rekomandimeve dhe masave korrigjuese si dhe verifikimi i implementimit të disa masave teknike", janë sanksionuar me gjobë:

Infrastruktura	**Numri**	**Të ardhura për buxhetin e shtetit nga gjobat**
Infrastruktura Kritike të Informacionit	4	**3 600 000 LEKË**
Infrastruktura të Rëndësishme të Informacionit	2	

Në kuadër të angazhimeve të vazhdueshme për forcimin e bashkëpunimit dhe ndarjen e informacionit në fushën e sigurisë kibernetike, ekspertët e AKCESK kanë marrë pjesë në një sërë takimesh të rëndësishme të organizuara nga NATO. Disa nga këto takime përfshijnë:

- MISP User Meeting – Maj 2023

Ky takim u fokusua në shkëmbimin e përvojave dhe praktikave më të mira në përdorimin e platformës MISP (*Malware Information Sharing Platform*), duke forcuar kështu kapacitetet tona në menaxhimin dhe ndarjen e të dhënave mbi kërcënimet kibernetike.

- Cyber Coalition 2023

Ky është një ndër ushtrimet më të mëdha të NATO-s në fushën e sigurisë kibernetike, i cili synon të përmirësojë ndërveprimin dhe koordinimin ndërmjet vendeve anëtare dhe partnerëve në rast të një sulmi kibernetik, Execution Tallin, 27 Nëntor – 1 Dhjetor 2023. Ky aktivitet përfshinte trajnime dhe ushtrime praktike, duke u fokusuar në përgatitjen dhe aftësimin e ekipeve tona për të përballuar sfidat aktuale dhe të ardhshme në fushën e sigurisë kibernetike.

Për sa më sipër, AKCESK ka bërë përparim të konsiderueshëm për harmonizimin e legjislacionit dhe praktikave të sigurisë kibernetike me standardet e Bashkimit Evropian. Gjatë këtij procesi, AKCESK ka vlerësuar dhe punuar për të transpozuar direktivat dhe rregulloret e BE-së si dhe është angazhuar për të rritur kapacitetet e tij dhe të infrastrukturave kritike dhe të rëndësishme të informacionit, që tregon angazhimin e thellë të qeverisë për të arritur një nivel të lartë të sigurisë kibernetike, në përputhje me objektivat e Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 dhe integrimin me praktikat më të mira ndërkombëtare.

3.1.2 POLICIA E SHTETIT (PSH)

Siç raporton Policia e Shtetit, lidhur me objektivin specifik të përmirësimit të kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend si dhe harmonizimin e tij me direktivat dhe rregulloret e Bashkimit Evropian, me urdhër të Ministrit të Brendshëm nr.494,

datë 30.12.2020 është miratuar "Strategjia për hetimin e krimeve kibernetike dhe Planit të Veprimit 2021-2025". Gjithashtu, me urdhër Nr.60, datë 15.01.2021 është miratuar nga Drejtori i Përgjithshëm i Policisë së Shtetit, "Programi i Punës i Task Forcës së Posaçme për zbatimin e Strategjisë për Hetimin e Krimeve Kibernetike" dhe "Planit i Veprimit 2021-2025". Në vijim është ngritur grup i punës ndërinstitucional për ndryshime në kodin penal. Gjithashtu, në zbatim të konventave ndërkombëtare, por dhe për shkak të funksionimit të tyre, është propozuar kalimi i disa veprave penale nga struktura të tjera tek strukturat e Hetimit të Krimit Kibernetik.

Bazuar në urdhrin nr. 974, datë 29.06.2023 të Drejtorit të Përgjithshëm të Policisë së Shtetit, janë përcaktuar veprat penale, objekt i punës në strukturat e Policisë së Shtetit me qëllim ndarjen e brendshme të punës së strukturave në nivel qendror dhe vendor. Me urdhër nr. 47, datë 14.04.2024, të Ministrit të Brendshëm "Për miratimin e strukturës dhe të organikës në nivel qendror, vendor dhe strukturat e veçanta të Policisë së Shtetit", është krijuar Drejtoria për Hetimin e Krimeve Kibernetike, në nivel qendror dhe nivel vendor.

Lidhur me objektivin specifik të përmirësimit të infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizimin dhe ekstremizmin e dhunshëm, në zbatim të urdhrit nr. 47, datë 14.04.2024 të Ministrit të Brendshëm "Për miratimin e strukturës dhe të organikës në nivel qendror, vendor dhe strukturat e veçanta të Policisë së Shtetit", me qëllim rritjen e kapaciteteve ekzistuese të mbrojtjes kibernetike është krijuar Drejtoria për Hetimin e Krimeve Kibernetike, në nivel qendror dhe nivel vendor.
Policia e Shtetit ka punuar për forcimin e kapaciteteve të kësaj strukture me shtrirje në të gjithë territorin e vendit, rritjen e kapaciteteve trajnuese si edhe rritjen e trajnimeve përkatëse në fushën e krimit kibernetik, rritjen e kapaciteteve logjistike të strukturave të Hetimit të Krimit Kibernetik, si dhe do vijojë të punojë më tej në këtë drejtim edhe gjatë vitit 2024.

Sa i përket bashkëpunimit ndërkombëtar, rritja e bashkëpunimit ndërmjet strukturave të hetimit të krimit kibernetik me partnerët në fushën ligj-zbatuese është pjesë e punës së vazhdueshme të Policisë së Shtetit, ku me krijimin e strukturës do t`i jepet edhe më shumë përparësi.

3.1.3 AGJENCIA KOMBËTARE E SHOQËRISË SË INFORMACIONIT (AKSHI)

Bazuar në raportimin shkresor, Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI) ka punuar për optimizimin e infrastrukturave të sigurisë, përmirësimin e procedurave dhe rregulloreve të sigurisë, si dhe për përmirësimin e sistemeve të mbrojtjes kibernetike dhe strukturave hardware.

AKSHI ka realizuar optimizimin e infrastrukturave të sigurisë duke zgjeruar infrastrukturën aktuale falë instalimit të agjentëve të sigurisë drejt institucioneve që kanë kërkuar ndihmën e AKSHI-t për monitorimin dhe reagimin ndaj incidenteve kibernetike. Gjithashtu, zgjerimi në aspektin teknik është kryer falë integrimit me platforma të ndryshme si inteligjenca kibernetike (*threat intelligence*) dhe mjedise testimi (*sandbox*). Organizimi si objekt i efiçencës në aftësinë

operative reaguese duke përdorur inteligjencën artificiale dhe *machine-learning* ka mundësuar automatizimin pa kërkuar ndërveprim human.

Si pjesë e modernizimit dhe funksionimit të CSIRT qeveritar, aktualisht AKSHI është i certifikuar me Standardet Ndërkombëtare ISO dhe gjithashtu po ndjek modelin SIM3, duke maturuar qeverisjen e CSIRT të tij, në vlerësim të performancës dhe dokumentimit. Vlen të theksohet se bashkëpunimi me ekipin përgjegjës SIM3 të Microsoft evidenton shtetin shqiptar ndër vendet e pakta evropiane që ndjekin këtë model. Gjithashtu NAIS GCSIRT (emërtuar CIRT qeveritar), është në proces listimi, duke aspiruar nivelin e certifikuar të Trusted Introducer dhe duke e radhitur kështu CSIRT qeveritar, si një partner mes CSIRT-ve në Bashkimin Evropian.

Në bashkëpunim me Microsoft është përmirësuar dokumenti i Rregullores së Sigurisë së Informacionit, duke integruar praktikat më të mira të sigurisë. Në bazë të ndjekjes së udhëzimeve të këtij dokumenti u është kërkuar personelit të AKSHIT në institucione, operatorëve ekonomikë dhe stafit të institucioneve zbatimi me rigorozitet i tij.

Gjithashtu, AKSHI ka ndjekur udhëzimet për menaxhimin dhe mitigimin e vulnerabiliteteve dhe informacioneve të ndryshme mbi aktivitetet e evidentuara, si dhe ka realizuar monitorimin e aplikimit të tyre me ndihmën e agjentëve të sigurisë të cilët analizojnë posturën e kompjuterëve fundorë, komponentët teknikë dhe sjelljet jo normale të përdoruesve.

Aktualisht Qendra Operacionale e Sigurisë së AKSHI-t dhe Ekipi i Reagimit ndaj Incidenteve Kibernetike monitoron dhe reagon ndaj incidenteve në hapësirën kibernetike qeveritare. Filozofia e cila është implementuar, Defense in Depth, siguron një mbrojtje me shumë shtresa. Synimi final është implementimi i parimit Zero Trust. Sa i përket objektivit lidhur me përmirësimin e strukturave hardware dhe ngritjen e sistemit të kontrollit të aksesit në rrjetin Gov Net, AKSHI ka marrë masat duke arritur realizimin në masën 90%.

Gjithashtu, AKSHI ka punuar për realizimin e hulumtimeve për forcimin e prioriteteve kombëtare, si një bazë për të parashikuar investimet për zhvillimin e sigurisë kibernetike. Në këtë kuadër janë publikuar punime të ndryshme shkencore në sajë të hulumtimeve shkencore në raport me posturën aktuale kibernetike dhe investimet që nevojiten për të ndërtuar një ekosistem të qëndrueshëm. Punimet janë prezantuar në konferenca shkencore kombëtare dhe ndërkombëtare si Qendra e Inovacionit të Sigurisë dhe të Mbrojtjes dhe Fakulteti i Ekonomisë i Universitetit të Tiranës.

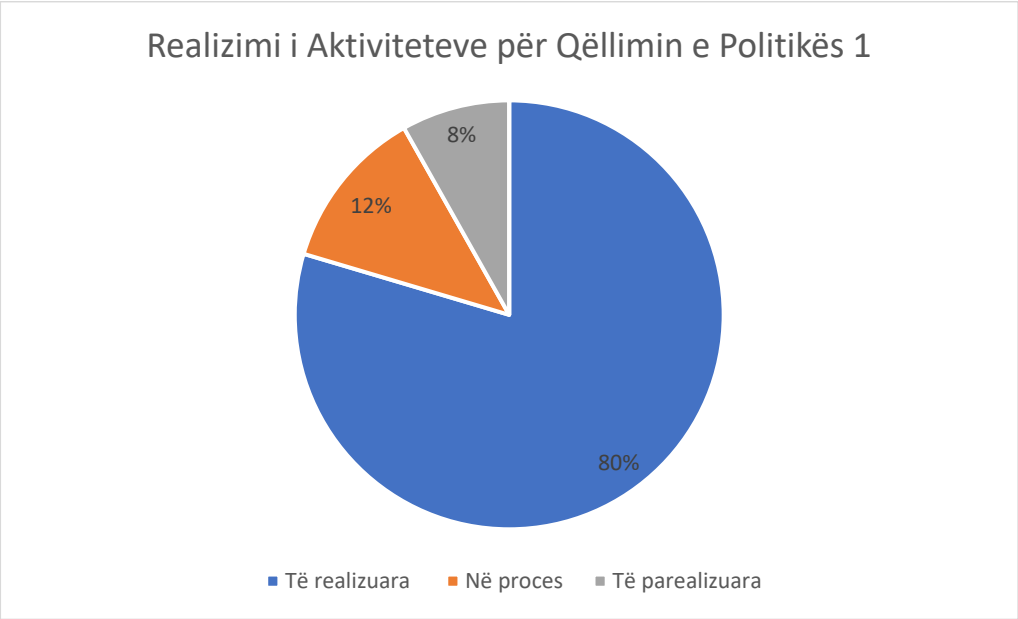
Për sa i përket disa prej objektivave të Strategjisë Kombëtare për Sigurinë Kibernetike që AKSHI punon për të përmbushur, marrëveshja e nënshkruar mes Këshillit të Ministrave dhe Microsoft kontribuon gjithashtu në realizimin e tyre.

Përmbledhje e Politikës 1

Duke iu referuar progresit të institucioneve të qeverisë shqiptare për qëllimin e politikës 1, të shënuar gjatë vitit 2023, është e qartë se Shqipëria po bën hapa pozitivë në harmonizimin e legjislacionit dhe praktikave të sigurisë kibernetike me standardet e Bashkimit Evropian. Përmirësimi i kapaciteteve, si dhe zbatimi i masave të sigurisë në infrastrukturave kritike janë të domosdoshme për të përballuar sfidat e sigurisë kibernetike, dhe AKCESK ka pasur rezultate të larta në këtë drejtim. Këto përpjekje, që dëshmojnë një angazhim të qëndrueshëm dhe të qartë për të garantuar një mjedis të sigurt kibernetik për të gjithë qytetarët, jo vetëm që rrisin sigurinë kombëtare, por gjithashtu forcojnë pozitat e Shqipërisë në arenën ndërkombëtare si një partner i besueshëm në adresimin e kërcënimeve kibernetike.

Realizimi i Aktiviteteve për Qëllimin e Politikës 1

Për Qëllimin e Politikës 1, rezulton se deri në vitin 2023, shkalla e realizimit të aktiviteteve është: aktivitete të realizuara 80% (39 aktivitete), aktivitete në proces 12% (6 aktivitete) dhe aktivitete të parealizuara 8% (4 aktivitete).



3.2 QËLLIMI I POLITIKËS 2. NDËRTIMI I NJË MJEDISI TË SIGURT KIBERNETIK DUKE EDUKUAR DHE NDËRGJEGJËSUAR SHOQËRINË NË NGRITJEN E KAPACITETEVE PROFESIONALE NË FUSHËN E SIGURISË SË INFORMACIONIT.

Objektivat e prioritetit fokusohen në:

- Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore;
- Rritja e ndërgjegjësimit dhe aftësive profesionale të institucioneve publike dhe private për sigurinë kibernetike;
- Rritje e ndërgjegjësimit të shoqërisë për sigurinë kibernetike dhe për kërcënimet kibernetike.

Për realizimin e objektivave të Qëllimit të Politikës 2, institucionet e përfshira në realizimin e Planit të Veprimit raportojnë si më poshtë vijon:

3.2.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK)

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike është angazhuar për zhvillimin dhe promovimin e një kulture të sigurisë kibernetike të qëndrueshme, duke punuar për rritjen e ndërgjegjësimit mbi rreziqet kibernetike dhe përmirësimin e mbrojtjes kibernetike, përmes zhvillimit të kapaciteteve të nevojshme njerëzore në fushën e sigurisë kibernetike.

Në këtë kuadër, AKCESK ka realizuar trajnime dhe fushata ndërgjegjësimi lidhur me sigurinë në internet, higjienën kibernetike, si dhe çështjet e sigurisë kibernetike për operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit (OIKI dhe OIRI), duke përfshirë institucionet publike dhe private.

AKCESK ka ndërmarrë hapa të rëndësishëm në kuadër të arritjes së objektivave për rritjen e kapaciteteve profesionale në fushën e sigurisë kibernetike nëpërmjet rishikimit të kurrikulave arsimore, të tilla si marrëveshja e nënshkruar me Akademinë e Forcave të Armatosura më datë 30.11.2023 mbi edukimin, hulumtimin dhe trajnimin e studentëve dhe stafit akademik në fushën e sigurisë kibernetike. Në kuadër të kësaj marrëveshje, në Janar 2024 u ngrit një grup pune i përbashkët ndërmjet AKCESK[2] dhe Akademisë së Forcave të Armatosura për të punuar për përmirësimin e kurrikulave në fushën e sigurisë kibernetike. Konkretisht, AKCESK është angazhuar për përmirësimin e kurrikulës lidhur me programin mësimor të ciklit të dytë të studimeve Master Profesional "Siguri kibernetike në fushën e mbrojtjes".

AKCESK në bashkëpunim me Akademinë e Forcave të Armatosura ka realizuar analizën e situatës aktuale të infrastrukturave kritike dhe të rëndësishme të informacionit të sektorit publik dhe privat duke identifikuar nevojat për përmirësime të mëtejshme në terma të kapaciteteve njerëzore dhe investimeve në fushën e sigurisë kibernetike. Përmes një pyetësori të hartuar dhe dërguar drejt 52 (pesëdhjetë e dy) subjekteve janë mbledhur të dhëna rreth burimeve njerëzore dhe aftësive të nevojshme në siguri kibernetike, me qëllim për të vlerësuar nevojat dhe mundësinë e përmirësimit të programit të Masterit Profesional në Siguri Kibernetike në fushën e mbrojtjes në Akademinë e Forcave të Armatosura (AFA).

AKCESK ka implementuar programe trajnimi dhe ndërgjegjësimi në fushën e sigurisë kibernetike për të edukuar fëmijët, të rinjtë, prindër e mësues si dhe punonjësit socialë mbi rreziqet që mund të hasen në hapësirën kibernetike, metodat e mbrojtjes si dhe institucionet ku mund të raportohen rastet e përmbajtjeve të dëmshme dhe të paligjshme.

[2] Marreveshje-bashkepunimi-1.pdf (aksk.gov.al)

Gjithashtu, gjatë vitit 2023, AKCESK ka shpërndarë materiale edukative, si dhe njoftime/lajme ditore mbi kërcënimet e mundshme kibernetike, incidentet kibernetike (të tilla si buletinet) në faqen zyrtare të Autoritetit[3], si dhe në rrjetet sociale.

Ngritja e kapaciteteve njerëzore në fushën e sigurisë kibernetike është një element kyç i Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planit të Veprimit 2020-2025. AKCESK u ka dhënë prioritet trajnimeve dhe përgatitjes së ekspertëve në këtë fushë, me qëllim përmirësimin e aftësisë për të parandaluar, zbuluar dhe trajtuar sulmet kibernetike. AKCESK ka punuar për rritjen e kapaciteteve profesionale të stafit të tij si dhe stafit përgjegjës për sigurinë kibernetike të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.

AKCESK ka realizuar fushata ndërgjegjësuese dhe trajnime me OIKI dhe OIRI të tilla si ushtrime tavoline, seminare, dhe stërvitje kibernetike. Gjatë vitit 2023, në aktivitetet e organizuara nga AKCESK janë trajnuar 250 individë nga 60 operatorë të infrastrukturave kritike dhe të rëndësishme të informacionit. Gjithashtu, AKCESK, në bashkëpunim me partnerët, është angazhuar në një seri iniciativash trajnuese të rëndësishme për të rritur kapacitetet në sigurinë kibernetike. Këto programe përfshijnë pjesëmarrjen e stafit në trajnime të ndryshme brenda dhe jashtë vendit, të dizajnuara për të adresuar një gamë sfidash në këtë fushë. Fokusi i trajnimeve ka qenë në mbrojtjen e infrastrukturave kritike të informacionit, menaxhimin e incidenteve dhe analizën e kërcënimeve. Qëllimi kryesor i këtyre trajnimeve ka qenë përmirësimi i njohurive dhe aftësitë e profesionistëve, ndërsa rritja e ndërgjegjësimit dhe ndërtimi i qëndrueshmërisë ndaj sulmeve kibernetike mbeten prioritete kryesore të AKCESK, të mbështetura nga ekspertiza e partnerëve.

Për sa më sipër, janë realizuar trajnime të specializuara për fuqizimin e kapaciteteve të stafit të AKCESK si vijojnë:

- CompTIA Security+;
- TAIEX workshop on Cybersecurity incident (case ID ETT 81753);
- KPMG – Hacker fundamentals";
- KPMG – Secure Coding;
- Threat Hunting Exercise;
- Cybexer Technologies – Technical Cybersecurity Threat Hunting Exercise- Cybersecurity Capacity Building Exercises for Albania, Montenegro and North Macedonia;
- Cyber Incident Response (CIR) training for Albanian critical Infrastructure Operators and Government Agencies, me mbështetjen e Catalisto LLC;
- Workshop"Governing Cyber Crisis";
- Cyber Tech Europe 2023;
- Security Operations Concepts and Practices Course, me mbështetjen e SEI;
- Cyber Defense Planning Engagement nga Instituti për Qeverisjen e Sigurisë i Shteteve të Bashkuara të Amerikës.

[3] Faqe zyrtare e AKCESK: www.aksk.gov.al

AKCESK ka realizuar gjithashtu trajnime të dedikuara me operatorët e infrastrukturave kritike të informacionit dhe infrastrukturave të rëndësishme të informacionit, të identifikuar për herë të parë në VKM Nr. 761, datë 12.12.2022.

Fokusi i trajnimeve ishte në çështjet e mëposhtme:

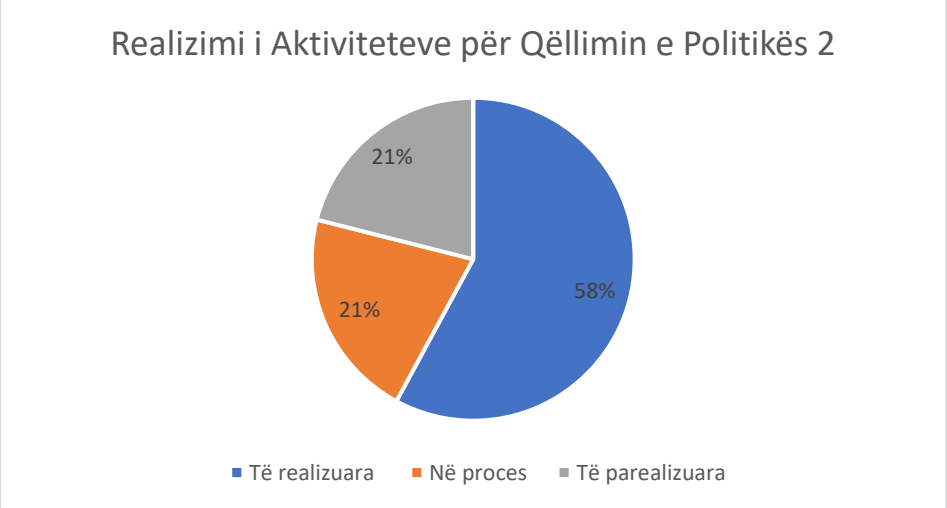
- Njohje me kuadrin ligjor të sigurisë kibernetike në Republikën e Shqipërisë;
- Plani i Ri Strategjik për Sigurinë Kibernetike;
- Menaxhimi i ciklit të jetës së CSIRT;
- Përfitimet e ngritjes së CSIRT;
- Kategorizimi i incidenteve kibernetike;
- Masat organizative dhe teknike të sigurisë që duhen implementuar nga OIRI dhe OIKI;
- Kontrollet e Sigurisë Kibernetike.

Përmbledhje e Politikës 2

Puna e kryer nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në kuadër të qëllimit të politikës 2 të Strategjisë Kombëtare për Sigurinë Kibernetike tregon një përkushtim të qartë dhe të vazhdueshëm ndaj forcimit të sigurisë kibernetike në të gjitha nivelet e shoqërisë. Nga trajnimet specifike për mbrojtjen e fëmijëve në internet, deri te përmirësimi i kurrikulave akademike dhe realizimi i fushatave të ndërgjegjësimit, AKCESK ka arritur të ndërtojë një bazë të fortë të njohurive që janë thelbësore për një mjedis digjital më të sigurt. Këto përpjekje jo vetëm që rrisin kapacitetet profesionale, por edhe forcojnë qëndrueshmërinë kibernetike të vendit, duke siguruar që të gjithë përdoruesit, nga fëmijët te profesionistët, të jenë më të aftësuar mbi kërcënimet në hapësirën kibernetike.

Realizimi i Aktiviteteve për Qëllimin e Politikës 2

Për Qëllimin e Politikës 2, rezulton se deri në vitin 2023, shkalla e realizimit të aktiviteteve është: aktivitete të realizuara 58% (11 aktivitete), aktivitete në proces 21% (4 aktivitete) dhe aktiviteteve të parealizuara 21% (4 aktivitete).



3.3 QËLLIMI I POLITIKËS 3. KRIJIMI I MEKANIZMAVE TË NEVOJSHËM PËR SIGURINË E FËMIJËVE NË HAPËSIRËN KIBERNETIKE, DUKE PËRGATITUR NJËKOHËSISHT BREZIN E RI TË AFTË PËR TË PËRFITUAR NGA PËRPARËSITË E TEKNOLOGJISË SË INFORMACIONIT DHE PËR TË PËRBALLUAR SFIDAT E ZHVILLIMIT

Objektivat e prioritetit fokusohen në:

- Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në internet;
- Parandalimi i abuzimit seksual të fëmijëve në internet nëpërmjet rritjes së ndërgjegjësimit dhe krijimit të hapësirave të sigurta për lundrimin në internet;
- Hetimi efektiv dhe sjellja para drejtësisë e autorëve të krimeve kibernetike ndaj fëmijëve, me fokus abuzimin dhe shfrytëzimin seksual;
- Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurtë të internetit nga fëmijët;
- Forcimi i bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në internet.

Për realizimin e objektivave të Qëllimit të Politikës 3, institucionet e përfshira në realizimin e Planit të Veprimit raportojnë si më poshtë vijon:

3.3.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK)

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka punuar në mënyrë të vazhdueshme në bashkëpunim me institucionet përgjegjëse për ngritjen e mekanizmave ndërvepruese ndërinstitucionale dhe organizimin e fushatave të ndërgjegjësimit dhe trajnimeve, për sigurinë *online* të fëmijëve dhe të rinjve, si detyrë funksionale e institucionit dhe në kuadër të përmbushjes së politikës numër 3, me objektiva të mirë-përcaktuara në planin e veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025.

Duke nisur nga viti 2021, Shqipëria nëpërmjet AKCESK si institucioni përgjegjës për mbrojtjen e fëmijëve dhe ndërgjegjësimin nga rreziqet e mundshme *online*, u angazhua për t'u bërë vendi i parë pilot për të zbatuar Projektin "*Creating a Safe and Prosperous Cyber Space for Children*" në bashkëpunim me Unionin Ndërkombëtar të Telekomunikacionit.

Projekti filloi zbatimin në shtator të vitit 2021 dhe u mbyll në Dhjetor të vitit 2023. Në këtë kuadër, AKCESK me mbështetjen e ITU, ka përgatitur dhe publikuar Udhëzuesit mbi Mbrojtjen e Fëmijëve Online (COP) në nivel kombëtar, organizimin e trajnimeve dhe workshop-eve, përgatitjen e materialeve të tjera dhe fushatave ndërgjegjësuese që synojnë rritjen e kapaciteteve dhe ndërgjegjësimin në nivel kombëtar të të gjithë aktorëve përgjegjës

për mbrojtjen e fëmijëve dhe të rinjve duke përshirë këtu prindërit, mësuesit, punonjësit e mbrojtjes sociale në shkolla, oficerët e sigurisë në shkolla si dhe përfaqësues nga bizneset.

Gjatë vitit 2023, AKCESK në bashkëpunim me Unionin Ndërkombëtar të Telekomunikacionit (ITU), në kuadër të pilotimit të Projektit Global "Krijimi i një Hapësire Kibernetike të Sigurt për Fëmijët", ka vazhduar me implementimin e fushatave të ndërgjegjësimit për të edukuar, fuqizuar dhe këshilluar fëmijët, punonjësit për mbrojtjen e fëmijëve dhe prindërit, lidhur me kërcënimet me të cilat mund të përballen në internet. AKCESK në bashkëpunim dhe me Agjencinë Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës (ASHDMF), realizoi disa trajnime *online* me temë "Mbrojtja e fëmijëve në internet dhe higjiena kibernetike", ku u trajnuan punonjësit e Njësive për Mbrojtjen e Fëmijëve në Bashkitë Dibër, Klos, Tiranë dhe Lushnje. Këto trajnime janë realizuar përkatësisht në datat 9, 10 dhe 13 Mars 2023.

AKCESK është pjesë e institucioneve raportuese për Shqipërinë për zbatimin e Konventës së Organizatës së Kombeve të Bashkuara, mbi të Drejtat e Fëmijës, ku gjatë punimeve të sesionit të 94-t, të Komitetit për të Drejtat e Fëmijës, mbajtur në Gjenevë, shtator 2023, raportoi mbi hapat konkretë të ndërmarrë për krijimin e një ekosistemi kibernetik të sigurt për fëmijët dhe të rinjtë. AKCESK, në këtë raportim theksoi nevojën e ndërgjegjësimit dhe mënyrat e mbrojtjes ndaj kërcënimeve të shtuara dhe të vazhdueshme që përballen fëmijët dhe të rinjtë në internet, si dhe nevojën e vazhdueshme për bashkëpunimin ndërinstitucional.

Workshop-i përmbyllës për projektin e përbashkët me ITU me temë, "Një dekadë ndërgjegjësim për sigurinë *online* të fëmijëve" u realizua në datë 6 dhjetor 2023, ku qëllimi kryesor ishte ndërgjegjësimi i grupeve të interesit dhe subjekte të sektorit të industrisë për krijimin e një hapësirë kibernetike të sigurt për fëmijët dhe të rinjtë.

Gjatë workshop-it, AKCESK prezantoi rezultatet e projektit dhe aktiviteteve të zhvilluara për implementimin e këtij projekti në të gjithë vendin. Pjesëmarrës ishin institucione shtetërore që kanë në fokus mbrojtjen e fëmijëve dhe të rinjve si Ministria e Arsimit dhe Sportit, Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës, Autoriteti i Komunikimeve Elektronike dhe Postare, Qendra e Parandalimit të Krimeve të të Miturve dhe të Rinjve, Policia e Shtetit, përfaqësues nga Ofruesit e Shërbimit të Internetit (ISP), si dhe organizata joqeveritare përfaqësuese të shoqërisë civile.

Gjatë diskutimeve përfaqësuesit e institucioneve, shoqërisë civile dhe biznesit treguan punën e tyre të vazhdueshme në mbrojtje të fëmijëve, ngritën problematika në lidhje me boshllëqet ligjore dhe nevojën e legjislacionit në fuqi për ndryshim, si dhe u angazhuan mbi krijimin e urave të mundshme të bashkëpunimit dhe krijimin e projekteve të vazhdueshme në të ardhmen.

Për sa më sipër arrihet në përfundimin se puna dhe angazhimet e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike dhe partnerëve të tij kanë sjellë rezultate konkrete pozitive në fushën e sigurisë *online* për fëmijët dhe të rinjtë në Shqipëri. Përmes projekteve të realizuara dhe trajnimeve të zhvilluara, AKCESK ka kontribuar në rritjen e ndërgjegjësimit dhe kapaciteteve të mbrojtjes kibernetike në nivel kombëtar, duke përfshirë një

gamë të gjerë aktorësh nga sektori publik dhe ai privat. Angazhimi i vazhdueshëm për të mbrojtur dhe edukuar grupet e ndjeshme, veçanërisht fëmijët dhe të rinjtë, në përballjen me sfidat kibernetike, shënon një hap të rëndësishëm drejt sigurisë në hapësirën kibernetike të vendit. Puna e bërë deri më tani shërben si bazë për iniciativa të ardhshme dhe përmirësimin e vazhdueshëm të politikave dhe praktikave mbrojtëse.

3.3.2 MINISTRIA E ARSIMIT DHE SPORTIT (MAS)

Bazuar në raportimin lidhur me procesin e monitorimit të zbatimit të masave të parashikuara në Planin e Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, Ministria e Arsimit dhe Sportit ka punuar lidhur me forcimin e kuadrit ligjor për rritjen e sigurisë së fëmijëve në internet, duke u angazhuar për hartimin e manualeve dhe udhëzimeve për përdorimin e internetit në mënyrë të sigurt.

Në kuadër të realizimit të objektivave të planit të punës për vitin 2023, Agjencia e Sigurimit të Cilësisë së Arsimit Parauniversitar (ASCAP) ka hartuar Manualin për Sigurinë në Internet[4], një material i cili ofron një paketë udhëzimesh dhe këshillash lidhur me promovimin e përdorimit të internetit në mënyrë të sigurt dhe efektive nga nxënësit dhe mësuesit. Qëllimi i këtij manuali ka të bëjë me njohjen e shërbimeve kryesore të internetit, si dhe sfidave dhe rreziqeve kryesore që vijnë nga përdorimi i tij në mënyrë të pasigurt. Manuali trajton në mënyrë të detajuar rreziqet kryesore që fëmijët mund të hasin përgjatë përdorimit të internetit, si: bullizmi kibernetik, ngacmimet seksuale, hakerimi i të dhënave personale, varësia nga lojërat *online*, etj. Ky material është publikuar në faqen zyrtare të ASCAP, si dhe është ndarë me mësues dhe drejtues rrjetesh.

Gjithashtu, lidhur me sigurinë kibernetike të nxënësve dhe mbrojtjen e tyre nga përmbajtjet e paligjshme dhe të dëmshme në institucionet arsimore parauniversitare janë në zbatim aktet e mëposhtme:

1. Udhëzimi i përbashkët midis Ministrisë së Arsimit, Sportit dhe Rinisë (MASR, sot MAS) dhe Ministrisë së Shëndetësisë dhe Mbrojtjes Sociale (MSHMS) nr. 658, datë 23.09.2019, "Për procedurat dhe veprimet që ndërmarrin strukturat arsimore, në bashkëpunim me strukturat e mbrojtjes së fëmijëve, në rastet kur në mjediset e institucionit arsimor parauniversitar konstatohet se një fëmijë është duke aksesuar në internet përmbajtje të paligjshme dhe/ose të dëmshme për moshën e tij"[5];
2. Udhëzimi nr. 34, datë 16.11.2018, "Për ndalimin e telefonit celular në institucionet arsimore parauniversitare, si nga mësuesi ashtu dhe nga nxënësi"[6];
3. Urdhri nr. 493, datë 30.07.2018, "Për mospërdorimin e telefonit celular gjatë procesit mësimor në shkolla".

Mbështetur dhe në pikën 15, të nenit 33 të Rregullores "Për funksionimin e institucioneve arsimore parauniversitare në Republikën e Shqipërisë", oficerët e sigurisë aktualisht

[4] https://www.ascap.edu.al/kurrikula/
[5] https://qbz.gov.al/eli/udhezim/2019/09/23/658/bc47bc07-8bcc-4337-a1d6-856d66877dab
[6] https://arsimi.gov.al/udhezim-nr-34-date-16-11-2018-per-ndalimin-e-telefonit-celular-ne-institucionet-arsimore-parauniversitare/

dokumentojnë punën e tyre sipas dokumentit "Praktika e punës së oficerëve të sigurisë në shkolla"[7] dhe përgatisin raportet periodike, si më poshtë:

1. Raporti i incidenteve/problematikave;
2. Raporti javor;
3. Raporti vjetor.

Në këto raporte jepen edhe problematikat dhe rastet për rreziqet kryesore që fëmijët mund të hasin përgjatë përdorimit të internetit, si: bullizmi kibernetik, ngacmimet seksuale, hakerimi i të dhënave personale dhe varësia nga lojërat online.

Në shkolla është ngritur rrjeti i bashkëpunimit me prindër, njësinë e mbrojtjes së fëmijëve (NJMF) për mbrojtjen e të miturve kundër dhunës kibernetike.

Sa i përket metodologjisë së mbledhjes së rasteve të incidenteve në shkolla, për oficerët e sigurisë në shkolla dokumenti i miratuar për realizimin e detyrave funksionale dhe mbledhjen e rasteve të incidenteve në shkolla është "Praktika e punës së oficerëve të sigurisë në shkolla".

Për shërbimin psiko-social (SHPS) janë miratuar dokumentet: "Praktika e punës së shërbimit psiko-social"[8] dhe "Parimet e përgjithshme etike të shërbimit psiko-social"[9] , të cilat trajtojnë situata të dhunës, bullizmit dhe abuzimit *online* në shkollë.

Metodologjia e mbledhjes së rasteve përmban:

1. Trajnime informuese me nxënësit dhe prindërit nga shërbimi psiko-social mbi rreziqet e përdorimit të pakontrolluar të internetit;
2. Krijimi i fletëpalosjeve dhe materialeve ndërgjegjësuese për informimin e nxënësve, prindërve dhe komunitetit lidhur me sigurinë kibernetike;
3 Zhvillimi i pyetësorëve nga ana e shërbimit psiko-social për kohën e shpenzimit në rrjete sociale dhe format e bullizimit që mund të shfaqen në to;
4. Trajtimi i bisedave informuese me nxënës/mësues/prindër mbi përdorimin e sigurt të internetit;
5. Trajnime sensibilizuese, kryesisht me nxënësit e klasave VII-IX, mbi tematikat e ekstremizmit të dhunshëm;
6. Tryeza të rrumbullakëta me pjesëmarrjen e aktorëve të ndryshëm, si mësues, nxënës, prindër, përfaqësues nga komuniteti, Policia e Shtetit etj., me tematikë: "Parandalimi i abuzimit seksual të fëmijëve në internet nëpërmjet rritjes së ndërgjegjësimit dhe krijimin e hapësirave të sigurta për lundrimin në internet";
7. Partneritet me prindërit për të thelluar komunikimin dhe mbështetjen për çështjet e bullizmit, ku rëndësi të veçantë ka pasur informimi dhe asistenca e prindërve në mënyrë që të arrijnë të trajtojnë këtë temë me fëmijët e tyre;
8. Vëzhgime në bashkëpunim me mësuesin kujdestar dhe shërbimin psiko-social të shkollave;
9. Pyetësor me nxënësit;

[7] https://www.ascap.edu.al/udhezuesi-per-praktiken-e-punes-se-oficereve-te-sigurise/
[8] https://www.ascap.edu.al/praktika-e-punes-se-sherbimit-psiko-social-shkollor/
[9] https://www.ascap.edu.al/parimet-per-etiken-profesionale-te-sherbimit-psiko-social-shkollor/

10. Këshillime individuale dhe në grup;
11. Fokus grupe.

Lidhur me raportet e institucioneve arsimore vendore përgjegjëse për arsimin parauniversitar Ministria e Arsimit dhe Sportit raporton se gjatë vitit 2023 janë hartuar raporte informuese nga Oficeri i Sigurisë dhe shërbimi psiko-social për parandalimin e dukurive negative duke evidentuar dhe ndërmarrë hapa në bashkëpunim me personelin mësimor dhe prindërit.

Në kuadër të punës edukative në institucione dhe planit të veprimtarive kundër ekstremizmit të dhunshëm, psikologët e shkollave në bashkëpunim me mësuesin koordinator të planit kundër ekstremizmit të dhunshëm në shkollë kanë organizuar veprimtari sensibilizuese mbi çështjen e sigurisë me nxënës dhe mësues me tematikë: "Përdorimi i internetit, rreziqet e sjelljeve ekstremiste në internet". Gjithashtu janë realizuar biseda informuese me tematikë: "Fëmijë të sigurt në internet dhe mbrojtja nga dhuna virtuale", të realizuara me nxënësit e klasave të arsimit të mesëm të ulët, me pjesëmarrjen e përfaqësuesve të Njësisë për Mbrojtjen e Fëmijëve, Koordinatores së Dhunës në Familje dhe psikologëve të institucioneve. Qëllimi kryesor i këtyre bisedave ka qenë informimi mbi domosdoshmërinë ligjore të respektimit të të drejtave të fëmijëve dhe mbrojtja e tyre nga çdo formë e dhunës.

Që nga viti shkollor 2021-2022 është ngritur dhe funksionon rrjeti profesional i mësuesve të TIK-ut, si dhe është ngritur grupi i koordinatorëve të shkollave, për kryerjen e raportit të vlerësimit për sigurinë kibernetike. Në kuadër të zbatimit të projektit të bashkëpunimit midis ASCAP dhe Institutit Shqiptar të Medias, për vitin 2023 janë trajnuar 10 shkolla, rreth 150 mësues mbi edukimin për median dhe informimin e arsimit të mesëm të ulët dhe arsimit të mesëm të lartë. Përveç njohurive të marra rreth botës së medias dhe informimit, janë diskutuar çështje të rëndësishme të cilat lidhen me sfidat dhe rreziqet në botën virtuale. Mësuesit janë njohur me kodet e sjelljes, rregullat e privatësisë dhe disa nga rreziqet kryesore që mund të hasen përgjatë përdorimit të internetit. Gjithashtu, janë inkurajuar mësuesit të përdorin metodat dhe mjetet bazë mësimore për të ndihmuar nxënësit të përdorin internetin në mënyrë të përgjegjshme dhe t'i bëjnë ata të vetëdijshëm për sfidat dhe rreziqet që vijnë nga përdorimi i tij. Gjithashtu, përgjatë vitit 2023 ky projekt është pilotuar edhe me drejtuesit e rrjeteve të shkencave sociale dhe biologji-kimisë, ku 120 drejtues rrjetesh kanë marrë pjesë në këto trajnime. Takimi i rrjetit profesional të mësuesve të TIK-ut realizohet 2 herë në muaj (1 takim i drejtpërdrejtë, 1 online) ku mësuesit diskutojnë, ndajnë eksperiencën dhe vlerësojnë nevojat.

Institucionet arsimore në vend aplikojnë filtra për të parandaluar aksesin e fëmijëve në faqe të papërshtatshme dhe të paligjshme, ku verifikimi i filtrave do të vijojë edhe gjatë vitit 2024. Në shkolla është ngritur gjithashtu grupi i koordinatorëve për raportin e vlerësimit për sigurinë kibernetike. Gjithashtu, hartohen raporte periodike të incidenteve nga oficerët e sigurisë ose punonjësit e shërbimit psiko-social dhe raportohen sipas dokumenteve përkatëse të punës. Në shkolla organizohen takime të mbyllura për të adresuar çështjen e bullizmit në rrjetet sociale në një mjedis të sigurt dhe të besueshëm, duke inkurajuar nxënësit të flasin lirshëm dhe të kërkojnë ndihmë.

Ministria e Arsimit dhe Sportit ka punuar për identifikimin, mbështetjen dhe promovimin e talenteve për të krijuar zgjidhje teknike që ndihmojnë në mbrojtjen dhe sigurinë online.

Metodologjia e ndjekur konsiston në hapat si vijon:
1. Identifikimi i nxënësve në shkolla nga mësuesit e TIK për prirjet që kanë në përdorimin e internetit dhe të kompjuterit;
2. Zhvillimi i konkurseve dhe projekteve me temë "Siguria në Internet". Dhënia e detyrave me shkallë të lartë vështirësie;
3. Zhvillimi i olimpiadës kombëtare çdo vit në lëndën e TIK-ut, si mundësi zbulimi të talenteve në TIK.

Siç raporton Ministria e Arsimit dhe Sportit, për monitorimin e aplikimit të metodologjisë më lart konsiderohen:
1. Realizimi i shpërndarjes së posterave sensibilizues mbi rrisqet që mund të sjellë përdorimi i internetit në mënyrë, jo të sigurtë;
2. Nxënësit të cilët kanë prirje në teknologji kanë trajnuar bashkëmoshatarët e tyre se si të mbrohen nga sulmet kibernetike;
3. Përcaktimi i nxënësve pjesëmarrës dhe fitues në olimpiadën kombëtare për lëndën e TIK-ut për secilën fazë.

Në kuadër të angazhimit për rritjen e sigurisë kibernetike dhe mbrojtjen e fëmijëve në internet, Ministria e Arsimit dhe Sportit, në bashkëpunim me institucione të tjera përkatëse, ka vënë në zbatim masa të rëndësishme ligjore dhe praktike. Realizimi i Manualeve për Sigurinë në Internet dhe zbatimi i udhëzimeve në mjediset arsimore janë pjesë e përpjekjeve për të ndërtuar një mjedis *online* më të sigurt për fëmijët dhe të rinjtë. Përmes trajnimeve, ndërgjegjësimit mbi rreziqet e internetit dhe promovimit të përdorimit të përgjegjshëm të teknologjisë, ky angazhim synon të mbrojë fëmijët nga përmbajtjet e dëmshme dhe të inkurajojë përdorimin e sigurt dhe efektiv të teknologjisë. Kjo qasje gjithëpërfshirëse dhe e koordinuar mbështet zhvillimin e një brezi të ri që është i edukuar dhe i pajisur për të përballuar sfidat e sigurisë në hapësirën kibernetike, duke kontribuar kështu në një shoqëri digjitale më të qëndrueshme dhe të sigurtë.

3.3.3 POLICIA E SHTETIT (PSH)

Policia e Shtetit ka punuar për **s**igurimin e mjeteve teknike që ndihmojnë strukturën e hetimit të krimeve kibernetike në Policinë e Shtetit në analizimin dhe zbulimin e rasteve të dhunës në rrjet veçanërisht lidhur me imazhet e abuzimit seksual me fëmijët si dhe krijimin e një grupi pune nga struktura e hetimit të krimit kibernetik së bashku me industrinë për të zgjidhur problemet e hetimit dhe identifikimit të personave të dyshuar për abuzim me fëmijët *online*, me fokus të veçantë identifikimin e përdoruesve fundorë nëpërmjet adresave IP.

Aktualisht, me vënien në zbatim të urdhrit nr. 47, datë 14.04.2023 të Ministrit të Brendshëm "Për miratimin e strukturës dhe të organikës në nivel qendror, vendor dhe strukturat e veçanta të Policisë së Shtetit" është krijuar Drejtoria për Hetimin e Krimeve Kibernetike, e cila në strukturën e saj ka Sektorin për Hetimin e Pornografisë me të Mitur në qendër, Seksionin për Hetimin e Pornografisë me të Mitur në Drejtorinë Vendore të Policisë Tiranë si dhe seksione në të gjitha qarqet e vendit ku mund të raportohen raste të cilat lidhen me krimet kibernetike.

Struktura e Krimit Kibernetik, që prej muajit dhjetor 2020 është pjesë e NCMEC (Qendra Kombëtare për Fëmijët e Humbur dhe të Shfrytëzuar), ku nëpërmjet raportimeve ditore, furnizohet me informacione mbi raste të dyshuara për vepra penale të lidhura me pornografinë më të mitur të cilat ndodhin në vendin tonë.

Gjithashtu, në vazhdimësi të procedurave të ndjekura nga Policia e Shtetit po punohet në lidhje me implementimin e sistemit AMBER. Sistemi "AMBER Alert" aktivizohet për rastet serioze të rrëmbimeve të fëmijëve, rastet e fëmijëve të humbur etj., si dhe shërben për të nxitur/galvanizuar komunitetin për të ndihmuar në kërkimin e fëmijëve të humbur/zhdukur. Puna për hetimin dhe evidentimin e autorëve të krimeve kibernetike ndaj fëmijëve është e vazhdueshme gjatë gjithë kohës.

Strukturat për Hetimet e Krimeve Kibernetike, gjatë vitit 2023, kanë marrë pjesë në takime sensibilizuese në shkolla dhe në tryeza të rrumbullakëta, në bashkëpunim dhe me OJF dhe organizata të tjera qeveritare, të cilat merren me sigurinë e fëmijëve, për parandalimin e abuzimit seksual të fëmijëve në internet, bullizmin, ruajtjen e të dhënave të tyre, etj.

Sa i përket krijimit të një grupi pune së bashku me industrinë, puna vazhdon dhe është ende në proces. Lidhur me të janë marrë iniciativa për bashkëpunimin me ISP në lidhje me shkëmbimin e informacionit. Në të njëjtën kohë, janë marrë iniciativa për bashkëpunimin me institucione publike dhe private në fushën e mbrojtjes së fëmijëve.

Përpjekjet e Policisë së Shtetit për luftimin e krimeve kibernetike, veçanërisht atyre që përfshijnë abuzimin seksual me fëmijët në internet, kanë rezultuar në krijimin e strukturave të specializuara dhe në implementimin e teknologjive të avancuara për zbulimin dhe trajtimin e këtyre rasteve. Angazhimi në përmirësimin e bashkëpunimit ndërmjet strukturave të hetimit kibernetik dhe industrisë, si dhe përfshirja në iniciativa kombëtare dhe ndërkombëtare tregojnë një vullnet të qartë për të adresuar këto sfida me seriozitet dhe efikasitet. Këto veprime jo vetëm që rrisin kapacitetin e zbulimit dhe ndjekjes së autorëve të këtyre krimeve, por gjithashtu kontribuojnë në ndërtimin e një mjedisi më të sigurt për fëmijët në hapësirën kibernetike, duke i dhënë prioritet mbrojtjes së tyre nga kërcënimet kibernetike.

3.3.4 MINISTRIA E SHËNDETËSISË DHE MBROJTJES SOCIALE (MSHMS)

Siç raporton Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës, për sa i përket forcimit të bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në internet, në kuadër të zbatimit të Agjendës Kombëtare për Mbrojtjen e të Drejtave të Fëmijëve 2021-2026, është hartuar raporti i monitorimit për vitet 2021-2022 në koordinim me ministritë e linjës, institucionet e pavarura dhe pjesëmarrjen e 120 fëmijëve, të cilët ishin pjesë e procesit dhe kanë dhënë kontribut në hartimin e këtij projekti.

Gjetjet dhe rezultatet e këtij raporti u paraqitën dhe u diskutuan në mbledhjen e Këshillit Kombëtar për mbrojtjen e të drejtave të fëmijëve, i cili u zhvillua më datë 2 nëntor 2023.Në takim morën pjesë edhe 19 fëmijë, ku ndër të tjera, në diskutimet e tyre një nga çështjet ishte edhe mbrojtja dhe siguria *online* gjatë lundrimit në internet.

Në nivel kombëtar janë 241 punonjës për mbrojtjen e fëmijëve në të gjitha bashkitë (61). Punonjësit për mbrojtjen e fëmijëve në të gjitha bashkitë kanë menaxhuar 1413 raste të fëmijëve për mbrojtje gjatë periudhës Janar -Shtator 2023.

Gjatë periudhës Janar -Dhjetor 2023 nga Linja Kombëtare ALO 116 111, kanë marrë këshillim *online* 1155 fëmijë dhe 386 raste janë referuar në institucionet publike përgjegjëse për trajtim dhe ndjekje.

Po kështu për rreth 60 raste të fëmijëve të dhunuar në mjedisin digjital janë dhënë këshillime dhe referuar për trajtim në institucionet përgjegjëse.

Në kuadër të bashkëpunimit për adresimin e nevojave të fëmijëve dhe garantimit të të drejtave të tyre, Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës dhe AKCESK, në bashkëpunim me organizatën "Nisma ARSIS", janë duke zbatuar programin "Një Hapësirë kibernetike më e sigurt për fëmijët dhe të rinjtë", në 4 bashki të vendit, Tiranë, Durrës, Elbasan dhe Krujë. Programi synon të promovojë të drejtat e fëmijëve në botën digjitale, duke ndërgjegjësuar aktorët publikë në këto bashki për një mjedis më të sigurt në lundrimin në internet.

Në periudhën nëntor-dhjetor 2023, janë zhvilluar takime në 4 bashkitë e mësipërme, ku kanë marrë pjesë 80 punonjës nga NJMF/PMF të njësive administrative punonjës sociale dhe psikologë të shkollave, mësues, oficerë të sigurisë në shkolla, punonjës policie, prokurorë dhe punonjës të policisë nga sektori i krimit kibernetik.

Në datën 20 nëntor 2023 në kuadër të ditës Ndërkombëtare për Fëmijët, Ministria e Shëndetësisë dhe Mbrojtjes Sociale, Ministri i Brendshëm, Ministrja e Arsimit dhe Sportit, Ministri i Shtetit për Rininë dhe Fëmijët si dhe përfaqësues të shoqërisë civile firmosën "Paktin Kombëtar kundër dhunës seksuale ndaj fëmijëve në Shqipëri", dokument që synon mbrojtjen e posaçme të fëmijëve nga dhuna seksuale me burim internetin, por edhe në jetën e përditshme.

Njëkohësisht në kuadër të Ditës Ndërkombëtare për Fëmijët në 20 Nëntor 2023, Ministria e Shëndetësisë dhe Mbrojtjes Sociale në Bashkëpunim me Agjencinë Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijëve , Ministrja e Shtetit për Rininë dhe Fëmijët, AKCESK, Shërbimi Social Shtetëror, partnerët kombëtare dhe Ndërkombëtare, organizuan një aktivitet ndërgjegjësues për të drejtat e fëmijëve. Në këtë aktivitet të organizuar në mjediset e qendrës "TUMO", tek Piramida fëmijët prezantuan projektet inovative, që ndjekin në qendër, duke dhënë mesazhe edhe për fëmijët e tjerë për të drejtat e tyre.

Puna e Agjencisë Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijëve, në bashkëpunim me institucione të ndryshme dhe organizata ndërkombëtare, tregojnë një angazhim të qëndrueshëm për mbrojtjen e fëmijëve në mjedisin *online* dhe fizik.

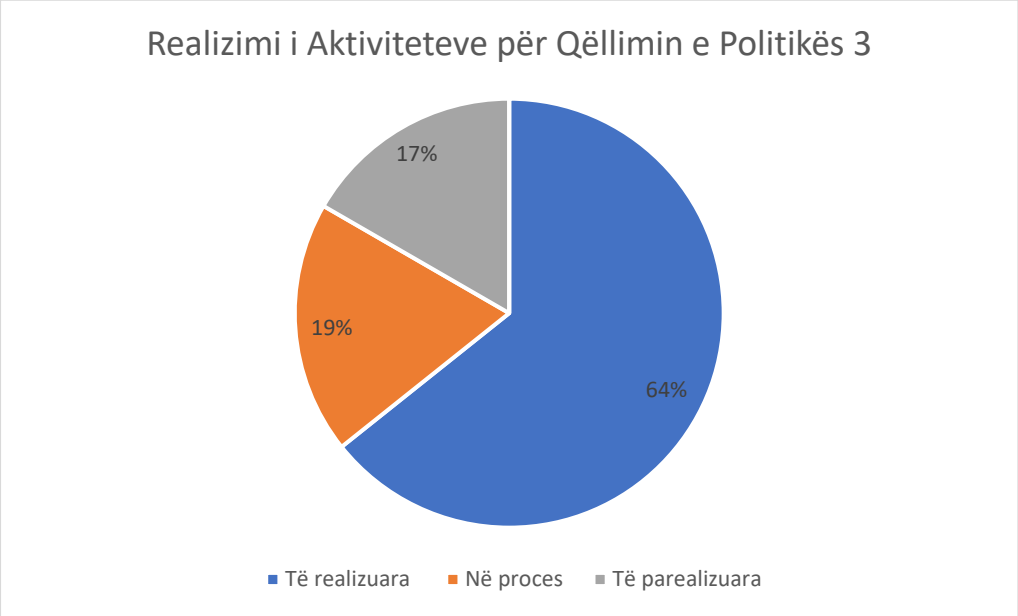
Përmbledhje e Politikës 3

Iniciativat e ndërmarra nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike dhe partnerët e tjerë institucionalë në kuadër të zbatimit të qëllimit të politikës 3 kanë kontribuar në ngritjen e një mjedisi më të sigurt kibernetik për fëmijët dhe të rinjtë në Shqipëri. Përpjekjet e përbashkëta për të rritur ndërgjegjësimin dhe kapacitetet mbrojtëse ndaj

sfidave *online*, përmes trajnimeve, udhëzimeve, dhe fushatave ndërgjegjësuese, kanë krijuar një bazë të fortë për të mbrojtur grupet më të ndjeshme të shoqërisë.

Realizimi i Aktiviteteve për Qëllimin e Politikës 3

Për Qëllimin e Politikës 3, rezulton se deri në vitin 2023, shkalla e realizimit të aktiviteteve është: aktivitete të realizuara 64% (27 aktivitete), aktivitete në proces 19% (8 aktivitete) dhe aktiviteteve të parealizuara 17% (7 aktivitete).



3.4 QËLLIMI I POLITIKËS 4. RRITJA E BASHKËPUNIMIT KOMBËTAR DHE NDËRKOMBËTAR NË FUSHËN E SIGURISË KIBERNETIKE ME PARTNERËT STRATEGJIKË

Objektivat e prioritetit konsistojnë në:

- Forcimi i bashkëpunimit institucional në nivel kombëtar;
- Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit.

Për realizimin e objektivave të Qëllimit të Politikës 4, institucioni përgjegjës për realizimin e Planit të Veprimit raporton si më poshtë vijon:

3.4.1 AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE (AKCESK)

AKCESK si Autoriteti përgjegjës për sigurinë kibernetike në nivel kombëtar, si dhe në përmbushje të detyrimeve ligjore e vizionit të Republikës së Shqipërisë për zhvillimin e teknologjisë së informacionit dhe komunikimit ka identifikuar partnerët në nivel kombëtar dhe

ndërkombëtar me të cilët Autoriteti mund të bashkëpunojë në kuadër të forcimit të sigurisë kibernetike si dhe ka zhvilluar procese dialogu me qëllim forcimin e bashkëpunimit.

Duke synuar forcimin e bashkëpunimit në nivel kombëtar dhe krijimin e sinergjive me qëllim adresimin dhe mbrojtjen ndaj rreziqeve kibernetike, Autoriteti ka hartuar e nënshkruar një sërë marrëveshjesh si me institucione publike ashtu edhe private brenda vendit.

Marrëveshjet e nënshkruara gjatë vitit 2023, janë si më poshtë vijojnë:

- Marrëveshje Bashkëpunimi me Shoqatën Shqiptare të Bankave (datë 06/02/2023);
- Marrëveshje Bashkëpunimi me Akademinë e Forcave të Armatosura (datë 07/12/2023);
- Marrëveshje Konfidencialiteti me Drejtorinë e Përgjithshme të Postës Shqiptare (datë 06/07/2023);
- Marrëveshje Bashkëpunimi dhe Konfidencialiteti me Operatorin e Sistemit të Transmetimit (datë 11/07/2023);
- Marrëveshje Konfidencialiteti me Kuvendin e Republikës së Shqipërisë (datë 16/10/2023);
- Marrëveshje Konfidencialiteti me Bankën e Parë të Investimeve (datë 23/11/2023);
- Marrëveshje Konfidencialiteti me Tirana Bank (datë 12.12.2023);
- Marrëveshje Konfidencialiteti me Union Bank (datë 19.07.2023);
- Marrëveshje Konfidencialiteti me Operatorin e Shpërndarjes së Energjisë Elektrike (OSHEE) (datë 13.07.2023);
- Marrëveshje Bashkëpunimi me Raiffeisen Bank (datë 03/11/2023).

AKCESK ka bashkëpunuar me Dhomën e Tregtisë dhe Industrisë Tiranë për organizimin e takimeve periodike me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

Rëndësi të veçantë i është dhënë bashkëpunimit me shoqërinë civile si Akademia e Studimeve Politike (ASP) me të cilën AKCESK organizoi projektin e përbashkët lidhur me ekstremizmin e dhunshëm dhe përmbajtjet e paligjshme në internet sipas kuadrit ligjor kombëtar dhe ndërkombëtar përkatës.

Në kuadër të bashkëpunimit kombëtar për forcimin e sigurisë kibernetike, AKCESK ka punuar për forcimin e komunikimit dhe besimit ndërmjet ekipeve publike dhe private të CERT dhe CSIRT përmes platformave të komunikimit të dedikuara. Në këtë kuadër është implementuar Sistemi i Menaxhimit dhe Raportimi të Incidenteve Kibernetike. Ky sistem i avancuar siguron një platformë të përbashkët komunikimi që lehtëson bashkëpunimin në raste incidentesh kibernetike dhe forcon besimin ndërmjet AKCESK dhe operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit që raportojnë incidentet kibernetike.

Implementimi i këtij sistemi jo vetëm që përmirëson efikasitetin dhe efektivitetin e reagimit ndaj incidenteve kibernetike, por gjithashtu ndihmon në ndërtimin e një ekosistemi më të sigurt dhe të besueshëm për të gjitha palët e interesuara. Autoriteti vijon të shkëmbejë informacione mbi përditësimet e sigurisë dhe Indikatorë të Kompromentimit nëpërmjet Sistemit të Menaxhimit dhe Raportimit të Incidenteve, sistem ky i ngritur që prej vitit 2019 për të lehtësuar

komunikimin e vazhdueshëm midis CSIRT-it Kombëtar dhe operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.

Sistemi i Menaxhimit dhe Raportimit të Incidenteve është një sistem i klasifikuar që përmban elementët e duhur të sigurisë për shkëmbime informacioni. Një tjetër hap i ndërmarrë është dhe ngritja e Platformës së Ndarjes së Informacioneve rreth Aktiviteteve Keqdashëse (MISP), e cila në nivel kombëtar, ka për qëllim ndarjen, ruajtjen dhe lidhjen e Indikatorëve të Kompromentimit (IoCs) të sulmeve të mundshme kibernetike dhe kërcënimeve, informacione të cilat lidhen me aktorët e kërcënimit kibernetik, vektorët e sulmeve etj.

AKCESK, për të garantuar një nivel sigurie më të lartë në nivel kombëtar në hapësirën kibernetike, është i angazhuar për përmbushjen me sukses të objektivave strategjikë edhe sa i përket rritjes së bashkëpunimit ndërkombëtar.

Përgjatë vitit 2023, AKCESK ka iniciuar takime me përfaqësues të autoriteteve homologe në Evropë me qëllim krijimin e kontakteve për shkëmbim informacioni, ndarjen e praktikave më të mira si dhe mundësinë për lidhjen e marrëveshjeve. Në këtë kuadër janë zhvilluar takime online me Italinë, Zvicrën, Norvegjinë dhe Letoninë.

Për të krijuar një rrjet komunikimi me qëllim shkëmbimin e informacionit dhe praktikave më të mira Autoriteti ka nënshkruar marrëveshje me institucione të mirënjohura ndërkombëtare si:

- Marrëveshje mirëkuptimi me 4IG (datë 20/01/2023);
- Marrëveshje bashkëpunimi me Drejtorinë Kombëtare të Sigurisë Kibernetike të Izraelit (datë 01/02/2023);
- Memorandum mirëkuptimi me Këshillin e Sigurisë së Emirateve të Bashkuara Arabe (datë 06.04.2023).

Autoriteti ka implementuar gjithashtu iniciativa të fokusuara kryesisht në rritjen e kapaciteteve duke integruar bashkëpunimin kombëtar dhe ndërkombëtar. Iniciativat dhe aktivitetet si konferenca, takime dhe trajnime në nivel kombëtar dhe rajonal kanë shërbyer edhe si ura komunikimi për bashkëpunimin dhe forcimin e besimit me operatorët e infrastrukturave të informacionit, publike dhe private, dhe komunitetin akademik. Për sa më sipër, AKCESK ka bashkëpunuar me partnerët ndërkombëtarë të cilët kanë në fokus sigurinë kibernetike si vijon:

- Unionin Ndërkombëtar të Telekomunikacionit (ITU);
- MITRE Corporation;
- Akademinë e Qeversisjes Elektronike (Electronic Governance Academy -eGA);
- Qendrën e Gjenevës për Qeverisjen e Sektorit të Sigurisë (DCAF);
- Forumin Global mbi Ekspertizën Kibernetike (GFCE), ku përgjatë 2023, AKCESK ndoqi procedurat e antëtarësimit, si anëtar me të drejta të plota në këtë organizatë;
- Counter Ransomware Initiative (CRI) ku AKSK në eventin Global "RSA Conference" në Prill 2023, AKSK shprehu interesin për tu bashkuar në CRI, duke u bërë shteti i 36 në botë anëtar;
- Shkollën Rajonale për Administratën Publike (ReSPA).

Autoriteti është angazhuar me pjesëmarrje aktive brenda dhe jashtë vendit në organizime të aktiviteteve të NATO-s, OSBE-së, OKB-së, BE-së, FIRST si në takime të nivelit politik dhe diplomatik, ashtu edhe në aktivitete si konferenca, stërvitje kibernetike dhe trajnime.

Konkretisht, në datat 6 - 10 Mars 2023, AKCESK ishte pjesë e punimeve të sesionit të IV të "*Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies*" në Kombet e Bashkuara. Fokusi i këtij sesioni ishin kërcënimet globale të sigurisë kibernetike, masat e ndërtimit të besimit, ngritja e kapaciteteve, si dhe normat e sjelljes së përgjegjshme të shteteve në hapësirën kibernetike. Në deklaratën e Shqipërisë u theksua progresi në harmonizimin e kuadrit ligjor me kornizën e Bashkimit Evropian si dhe arritjet në lidhje me ngritjen e CSIRT Kombëtar; trajnimeve për rritje kapacitetesh të CSIRT-eve sektoriale; konsolidimin e kapaciteteve për diplomacinë kibernetike dhe qeverisjen kibernetike; trajnimeve dhe fushatave të ndërgjegjësimit për administratën publike, industrinë, fëmijët e të rinjtë; si dhe trajtimin e temave të sigurisë kibernetike në kurrikulat arsimore.

Në mënyrë të veçantë, pjesëmarrja aktive në takimet e NATO-s për zbatimin e standardeve dhe rregulloreve ndërkombëtare në kuadër të sigurisë kibernetike është një komponent kyç për përmirësimin e mbrojtjes kibernetike. Në këtë kuadër, janë realizuar takime në Bruksel dhe Mons ku është diskutuar dhe demonstruar përdorimi i platformës MISP (*Malware Information Sharing Platform*) për shkëmbimin e informacionit mbi kërcënimet dhe incidentet kibernetike. Këto takime kanë ndihmuar në rritjen e bashkëpunimit dhe shkëmbimit të informacionit midis vendeve anëtare të NATO-s, duke përmirësuar përgjigjen ndaj kërcënimeve kibernetike dhe sigurinë kibernetike në tërësi.

Gjithashtu AKCESK ka rol të rëndësishëm në forcimin e bashkëpunimit dhe shkëmbimin e informacionit me NATO, OSBE dhe organizata / forume të tjera ndërkombëtare. Në sajë të ndërveprimit dhe bashkëpunimit me NATO-n, AKCESK ka arritur të jetë pjesë dhe të përdorë platformën NATO-MISP, vënë në dispozicion nga NATO për Shqipërinë, e cila kryen ndërveprim me organizatat ndërkombëtare për raportimin e incidenteve dhe Indikatorëve të Kompromentimit, të ndodhura në infrastrukturat e informacionit në nivel global. Kjo bën të mundur që AKCESK, në rolin e CSIRT-it Kombëtar, të informojë dhe të ndërgjegjësojë në kohë reale infrastrukturat e informacioni rreth incidenteve të ndodhura dhe raportuara. Gjithashtu, është realizuar bashkëpunimi i të gjithë aktorëve relevantë në procesin e zhvillimit dhe bashkimit të normave të sigurisë, standardizimin e bashkëpunimit, si dhe përcaktimin dhe vendosjen e nivelit të detyrueshëm të mbrojtjes së subjekteve që menaxhojnë incidentet kibernetike.

Për sa i përket anëtarësimit dhe pjesëmarrjes në aktivitete dhe iniciativa të ndryshme ndërkombëtare në fushën e sigurisë kibernetike, përfaqësuesit e AKCESK kanë marrë pjesë në eventet e mëposhtme:

- FIRST/DCAF Technical Colloquium | Balkan Cybersecurity Days 2023 - Ohrid, MK;

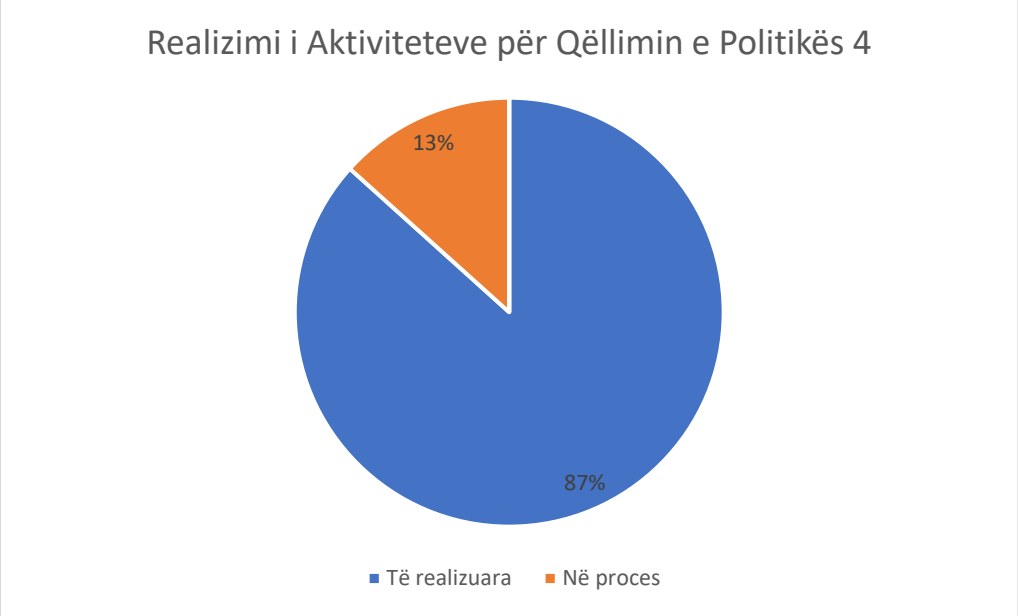
-TF-CSIRT Meeting & 2023 FIRST Regional Symposium for Europe - Bilbao, ES.

Përmbledhje e Politikës 4

AKCESK ka forcuar bashkëpunimin dhe rritur shkëmbimin e informacionit në nivel kombëtar dhe ndërkombëtar, duke hartuar dhe nënshkruar marrëveshje të ndryshme me qëllim të përmirësimit të sigurisë kibernetike. Ky bashkëpunim mundëson shkëmbimin e njohurive dhe përvojave të çmuara, si dhe ndërtimin e një mjedisi të sigurt kibernetik. Përmes angazhimit aktiv në takime dhe konferenca ndërkombëtare, si dhe nëpërmjet implementimit të standardeve ndërkombëtare, teknologjive të avancuara dhe masave të sigurisë, AKCESK kontribuon në një përgjigje më efikase dhe të koordinuar ndaj incidenteve kibernetike, duke e bërë Shqipërinë një shtet që angazhohet maksimalisht në sigurinë kibernetike në nivel kombëtar dhe ndërkombëtar.

Realizimi i Aktiviteteve për Qëllimin e Politikës 4

Për Qëllimin e Politikës 4, rezulton se deri në vitin 2023, shkalla e realizimit të aktiviteteve është: aktivitete të realizuara 87% (13 aktivitete), aktivitete në proces 13% (2 aktivitete) dhe aktiviteteve të parealizuara 0% (0 aktivitete).



4. REKOMANDIME

✓ **Rritja e investimeve në teknologji dhe infrastrukturë**

-Shtimi i investimeve në teknologjitë më të fundit të sigurisë kibernetike për të mbrojtur më mirë infrastrukturat kritike dhe të rëndësishme të informacionit.

-Forcimi i kapaciteteve të Qendrës Kombëtare Operacionale të Sigurisë Kibernetike SOC, për të përfshirë kapacitete të avancuara të monitorimit dhe përgjigjes ndaj incidenteve duke mbuluar të gjitha infrastrukturat kritike dhe të rëndësishme në nivel kombëtar.

-Krijimi i kushteve optimale të punës për funksionimin e CSIRT-eve, për të lehtësuar përmbushjen e detyrave të tyre me efektivitet, me qëllim garantimin e sigurisë kibernetike në infrastrukturat kritike e të rëndësishme të informacionit.

✓ **Përmirësimi i kuadrit ligjor dhe rregullator, në linjë me acquis e Bashkimit Evropian**

-Miratimi i projektligjit " Për identifikimin elektronik dhe shërbimet e besuara".

-Hartimi dhe miratimi i akteve nënligjore për zbatim të ligjit të ri nr. 25/2024 "Për sigurinë kibernetike" që transpozon direktivën NIS2.

-Harmonizimi i mëtejshëm i legjislacionit kombëtar me direktivat dhe standardet e Bashkimit Evropian.

-Hartimi dhe miratimi i rregullores për ofrimin e internetit të sigurt në hapësirat publike dhe me gjerë.

✓ **Miratimi dhe zbatimi i Plani i Veprimit 2024-2025 të Strategjisë Kombëtare për Sigurinë Kibernetike**

-Miratimi i Planit të Veprimit i hartuar për t'iu përgjigjur dinamikës së kërcënimeve kibernetike dhe zhvillimeve teknologjike, si dhe zbatimi i masave të reja të parashikuara për periudhën 2024-2025.

✓ **Ndërgjegjësim dhe edukim i vazhdueshëm**

-Zgjerimi i programeve të ndërgjegjësimit për publikun e gjerë për rëndësinë e sigurisë kibernetike dhe masat mbrojtëse që individët mund të marrin.

-Integrimi i kurrikulave të sigurisë kibernetike në sistemet arsimore, nga arsimi bazë deri te ai universitar.

✓ **Zhvillimi i kapaciteteve dhe trajnimeve profesionale**

-Shtimi i programeve të trajnimit për zhvillimin e aftësive të sigurisë kibernetike në të gjitha nivelet e institucioneve publike dhe private.

-Rekrutimi dhe trajnimi i talenteve të reja në fushën e sigurisë kibernetike përmes bursave dhe programeve të specializuara.

✓ **Përgjigje dhe menaxhim i incidenteve**

-Zhvillimi dhe zbatimi i një plani të përgjithshëm dhe të koordinuar për menaxhimin e incidenteve kibernetike që përfshin të gjithë aktorët kyç kombëtarë dhe ndërkombëtarë.

-Përmirësimi i kapaciteteve të reagimit të shpejtë dhe efektiv ndaj incidenteve për të parandaluar dhe minimizuar efektin e tyre.

- ✓ **Forcimi i bashkëpunimit ndërkombëtar**

-Forcimi dhe promovimi i bashkëpunimit ndër-sektorial në sigurinë kibernetike për të siguruar zbatimin e plotë të Strategjisë Kombëtare për Sigurisë Kibernetike.

-Zgjerimi i marrëveshjeve të bashkëpunimit me organizata ndërkombëtare dhe shtete të tjera për të shkëmbyer njohuri, teknologji dhe praktika më të mira.

-Pjesëmarrje më aktive në forume dhe iniciativa ndërkombëtare për të promovuar sjelljen e përgjegjshme të shteteve në hapësirën kibernetike, kontribuar në përcaktimin e normave dhe masave të ndërtimit të besimit, si dhe rritur aftësinë e përgjigjes ndaj kërcënimeve transnacionale.