REPUBLIKA E SHQIPËRISË
KËSHILLI I MINISTRAVE
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Raport Përfundimtar

“DOKUMENTI I POLITIKAVE PËR SIGURINË KIBERNETIKE 2015-2017”

Mars 2018

PASQYRA E LËNDËS

I PËRMBLEDHJE EKZEKUTIVE 3

Kuadri ligjor dhe institucional 4

Vizioni 4

II METODOLOGJIA E MONITORIMIT 5

III PROGRESI I ZBATIMIT TË OBJEKTIVAVE STRATEGJIKË 5

IV PËRFUNDIME 17

I. PËRMBLEDHJE EKZEKUTIVE

Këshilli i Ministrave në datë 02.12.2015 miratoi me VKM-në Nr. 973 , "Dokumentin e Politikave për Sigurinë Kibernetike 2015-2017".

Qëllimi i këtij Dokumenti Politikash është të rishikojë dhe të koordinojë detyrimet që lindin nga angazhimet e marra për një hapësirë kibernetike të sigurt me qëllim që të sigurohet përmbushja e përgjegjësive nga të gjithë aktorët në mënyrë të koordinuar. Në këtë mënyrë mund të garantohet zhvillimi i mëtejshëm i shoqërisë së informacionit si një ambient i sigurt, i besueshëm dhe i hapur si dhe promovimi i vlerave dhe mundësive të ofruara nga përdorimi i hapësirës kibernetike.

Dokumenti i politikave të Sigurisë Kibernetike u hartua në mbështetje të programit të ri të investimeve në TIK të qeverisë shqiptare (Përmirësimi i shërbimeve ndaj publikut, Një shoqëri informacioni e sigurtë si dhe Strategjinë e Sigurisë Kombëtare 2014-2020) si edhe në këto dokumentet strategjikë :

- Axhenda Dixhitale e Shqipërisë (2014 - 2020)
- Strategjia për Sigurinë Kibernetike e Bashkimit Evropian: Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur (ang. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace),

Dokumenti pas një analize të situatës dhe zhvillimeve aktuale, përcaktoi vizionin dhe objektivat e zhvillimit për periudhën 2015-2017 si dhe drejtimet kryesore të politikave që do të ndiqen për realizimin e këtyre objektivave.

Dokumenti shoqërohet edhe me planin e veprimit në të cilin u përcaktuan aktivitetet që parashikohen të ndërmerren nga institucionet përgjegjëse, afatet për implementim, kostot e mundshme etj,

Gjatë muajit Dhjetor 2017, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në kuadër të përmbylljes së monitorimit të planit të veprimit, kërkoi raportim nga institucionet përgjegjëse, lidhur me përmbushjen e angazhimeve respektive.

Ky Dokument është gjithashtu në linjë me Agjendën Dixhitale për Evropën 2020 si dhe në linjë me Strategjinë për Sigurinë Kibernetike të Bashkimit Evropian: Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur (ang. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace).

Strategjia Ndër-sektoriale për Shoqërinë e Informacionit 2008-2013 (SNSHI) e miratuar me VKM Nr. 59, dt. 21.1.2009 përveçse përbën dokumentin strategjik që përcaktonte drejtimet kryesore dhe objektivat e zhvillimit në fushën e shoqërisë së informacionit për periudhën 2008 – 2013 ishte edhe dokumenti i vetëm ku përmendej shkurtimisht siguria kibernetike si një nga fushat që duhej konsideruar me prioritet për shkak të vizionit të Qeverisë shqiptare për të rritur e zhvilluar e-qeverisjen përmes ofrimit të e-shërbimeve.

Rëndësi të veçantë merr inicimi i ndryshimeve ligjore në mënyrë që të ofrohet mbrojtje e përshtatshme për përdoruesit, për të rritur besimin e tyre në teknologjitë e informacionit dhe për të inkurajuar përdorimin e avancuar dhe të sigurt të TIK-ut.

Vlerësohet si tejet e nevojshme marrja e veprimeve dhe masave specifike për të ndërgjegjësuar shoqërinë lidhur me rreziqet potenciale në fushën e sigurisë së rrjeteve dhe sistemeve për eliminimin e këtyre rreziqeve, përfshirë mbrojtjen e fëmijëve nga përmbajtjet e paligjshme në hapësirën kibernetike.

1.1 Kuadri ligjor dhe institucional

Zhvillimi i shpejtë i TIK kushtëzohet dhe nga përshtatja e legjislacionit përkatës të nevojshëm. Në përgjithësi Shqipëria është në pajtueshmëri me detyrimet që rrjedhin nga MSA-ja në këtë fushë. Ka disa ligje që rregullojnë ndjekjen penale të krimeve kompjuterike në Republikën e Shqipërisë si: Ligji Nr. 8888 i datës 25.04.2002 ,"Për Ratifikimin e Konventës për Krimin Kibernetik" është reflektuar në Kodin Penal si dhe Ligji Nr. 9262 i datës 29.07.2004 "Për Ratifikimin e Protokollit shtesë të Konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike" sërish është reflektuar në Kodin Penal.

1.2 Vizioni

Për një hapësirë kibernetike më të sigurtë, më të besueshme dhe më të qëndrueshme për qytetarët, biznesin dhe qeverinë në mbështetje të zhvillimit ekonomik dhe social të Shqipërisë.

Hapësira kibernetike duhet parë si një fushë shumë dimensionale, me shumë shtresa dhe gjerësi territoriale përtej kufijve kombëtarë.

Në përputhje me zhvillimet dhe iniciativat do të ndërmerren hapat e nevojshëm për të analizuar, përshtatur dhe plotësuar legjislacionin në fushën kibernetike. Në mënyrë të vazhdueshme do të bëhet vlerësimi i praktikave më të mira botërore, rekomandimeve dhe iniciativave ndërkombëtare të fushës në mënyrë të veçantë ato të NATO dhe BE, duke përshtatur masat në fushën e sigurisë kibernetike në përputhje me angazhimet e marra ndaj partnerëve ndërkombëtarë. Nëse do të konsiderohet e nevojshme do të bëhet përshtatja dhe miratimi i tyre duke garantuar kështu forcimin e sigurisë kibernetike dhe luftën kundër krimit kibernetik.

II. METODOLOGJIA E MONITORIMIT

Vlerësimi i realizimit të objektivave të këtij dokumenti politikash, u realizua duke monitoruar në mënyrë periodike realizimin e aktiviteteve të përcaktuara për periudhën 2015-2017, dhe indikatorët që shoqërojnë secilin aktivitet.

Monitorimi i dokumentit të politikave është mbështetur në këto faza kryesore:

a) Raportimi i institucioneve mbi zbatimin e aktiviteteve për të cilat janë përgjegjëse

b) Monitorimi i indikatorëve

Me qëllim realizimin e objektivave të dokumentit të politikave, metodologjia e monitorimit ka konsistuar në komunikimin e vazhdueshëm me institucionet përgjegjës, monitorimin e realizimit të angazhimeve të marra.

III. PROGRESI I ZBATIMIT TË OBJEKTIVAVE STRATEGJIKË

Objektivi 1. Plotësimi i kuadrit ligjor/rregullator në fushën e sigurisë kibernetike.

- Draftimi i Ligjit për Sigurinë Kibernetike.
- Draftimin e akteve nënligjore për sigurinë kibernetike.

Aktivitetet për realizimin e objektivit do të fokusohen kryesisht në:

Për realizimin e objektivit, institucionet e përfshira raportuan sa më poshtë:

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) ka raportuar se në bashkëpunim me institucionet e tjera përgjegjëse (MIAP, AKSHI, AKCE, DSIK, MM, MPB) ka hartuar draftligjin për Sigurinë Kibernetike i cili u miratua në Kuvend në datën 26.1.2017.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike AKCESK (bashkim i ALCIRT me AKCE, Maj 2017), gjatë vitit 2017, ka draftuar aktet nënligjore në zbatim të ligjit për Sigurinë Kibernetike;

- ✓ Rregullore për Menaxhimin e Firewall-eve
- ✓ Rregullore për Menaxhimin e Log-eve Digjitale në Administratën Publike
- ✓ Udhëzim për Masat e Sigurisë për Bazat e të Dhënave Shtetërore
- ✓ Rregullore për Administrimin e Portalit Online për Mbylljen e Aksesit të Faqeve të Internetit me Përmbajtje të Paligjshme

Gjithashtu janë draftuar dhe më pas miratuar;

- ✓ VKM 69 datë 27.1.2016, "Për miratimin e rregullores “Për Identifikimin Elektronik dhe Shërbimet e Besuara";
- ✓ Ndryshim i Ligjit Nr. 9880, datë 25.2.2008, "Për Nënshkrimin Elektronik";
- ✓ Ndryshimi i Ligjit 10273 Për dokumentin elektronik;
- ✓ VKM Nr. 71, datë 27.1.2016, Për disa ndryshime në vendimin Nr. 503, Datë 13.5.2009, të Këshillit të Ministrave, "Për miratimin e tarifave dhe shërbimeve për shërbimet që ofrohen nga Autoriteti Kombëtar Për Certifikimin Elektronik";
- ✓ Udhëzim Nr. 3, datë 02.02.2016 "Për vërtetimin e kopjes në letër të dokumentit elektronik nëpërmjet vendosjes së një apo më shumë kodeve dy dimensionale nga institucionet publike"
- ✓ Udhëzim Nr.4 Mbi procedurat e identifikimit dhe vulave elektronike

Shtabi i Përgjithshëm i Forcave të Armatosura ka raportuar se në kuadër të objektivit të parë strategjik ka ngritur pranë Agjencisë së Sistemeve të Ndërlidhjes dhe Informacionit (ASNI) të strukturës për Mbrojtjen Kibernetike dhe Kriptografinë.

Gjithashtu, Shtabi i Përgjithshëm i Forcave të Armatosura raportoi se ka hartuar sa më poshtë:

- ✓ Procedura standarde të punës për hapje/dhënie aksesi në rrjetin e klasifikuar dhe atë të paklasifikuar të Forcave të Armatosura, (viti 2015).
- ✓ Procedura standarde e punës për trajtimin e incidenteve kibernetike në rrjetet kompjuterike të Forcave të Armatosura, (viti 2016).
- ✓ Bazuar në raportet e njësisë së Analizës mbi sigurinë kibernetike të NATO-s, është hartuar një, Qarkore, për trajtimin e sulmeve kibernetike në rrjetet kompjuterike të FA si dhe përmbledhje mbi rreziqet e incidenteve kibernetike, (viti 2016, 2017).
- ✓ Procedura Standarde Veprimi “Për vërtetimin, identifikimin, sigurinë dhe menaxhimin e fjalëkalimeve nga përdoruesit e rrjeteve kompjuterike të SHPFA”, (viti -2017).
- ✓ Udhëzimi “Për ruajtjen, sigurinë, administrimin dhe inventarizimin e radiove të komunikimit taktik të cilat sigurojnë komunikim deri në nivelin NATO-Sekret”, (viti -2017).
- ✓ Udhëzimi “Për sigurinë fizike, administrimin dhe përdorimin e materialeve kriptografike në stërvitje ose misione jashtë vendit”, (viti -2017).
- ✓ Procedura e operimit të sigurt në rrjetin e klasifikuar të SHPFA, (Viti-2017).
- ✓ Udhëzimi mbi mënyrën e instalimit të pajisjeve të Teknologjisë së Informacionit dhe Komunikimit në objektet që përpunojnë informacion të klasifikuar, (viti-2017).
- ✓ Është miratuar dokumenti për akreditimin e radiove RF-5800 “HARRIS” dhe certifikimin e kompjuterëve “PANASONIC CF-29/30” për të operuar me R/Sist. RF-5800 deri dhe përfshirë nivelin konfidencial. Akreditimi është bërë nga DSIK.
- ✓ Certifikimin i rrjetit të klasifikuar të FA deri dhe përfshirë nivelin konfidencial. Akreditimi është bërë nga DSIK
- ✓ Udhëzimet dhe procedurat e sipërpërmendura rishikohen dhe përditësohen në përputhje me Politikat kombëtare dhe ato të NATO-s

Objektivi 2. Forcimi i kuadrit institucional

Aktivitetet për realizimin e objektivit do të fokusohen kryesisht në:

- Investime për infrastrukturat e sigurisë në rrjetet/sistemet shtetërore
- Të shtohen infrastrukturat e sigurisë në rrjetet/sistemet shtetërore
- Krijimi i portalit të ndërgjegjësimit me fokus sigurinë kompjuterike, fëmijët në internet, biznesin, këshilla sigurie dhe artikuj.
- Krijimi i një dege master në siguri kibernetike

Për realizimin e objektivit, institucionet e përfshira raportuan sa më poshtë:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), ka raportuar se në kuadër të këtij objektivi, ka përfunduar;

- ✓ Draft rregullore mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë,
- ✓ Draft rregullore për kundërmasat ndaj incidenteve,
- ✓ Draft urdhër për Përcaktimin e rasteve dhe kritereve për heqjen e detyrimit të konfidencialitetit për të dhënat e përpunuara gjatë incidenteve të sigurisë kibernetike.

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI) raportoi se ka kryer investime për infrastrukturat e sigurisë në rrjetet/sistemet shtetërore. Ngritja e BCC-ve (business continuity center) dhe DRC-ve (disaster recovery center) për rrjetet/sistemet shtetërore gjatë vitit 2016, AKSHI ka nënshkruar kontratat përkatëse lidhur me ngritjen e BCC-ve (business continuity center) dhe DRC-ve (disaster recovery center) për rrjetet/sistemet shtetërore.

Drejtoria e Përgjithshme e Tatimeve raportoi se është në proces përfundimi përsa i përket shtimit të infrastrukturave të sigurisë në rrjetet/sistemet shtetërore. Investime në hardware dhe software të automatizuara si masa proaktive dhe reaktive për të siguruar sistemet që administrojnë.

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) raportoi se ka krijuar portalin e ndërgjegjësimit me fokus sigurinë kompjuterike, fëmijët në internet, biznesin, këshilla sigurie dhe artikuj. ALCIRT ka krijuar faqen në facebook ¨cyberalbania¨ me

objektiv edukimin për një shoqëri dixhitale të sigurtë duke përdorur internet të sigurtë në shtëpi, punë, shkollë etj.

Universiteti i Tiranës, raportoi për këtë objektiv se ka krijuar një degë master në siguri kibernetike me objektiv përgatitjen e një brezi të ri specialistësh të mirëfilltë për sigurinë kibernetike.

Objektivi 3. Rritja e ndërgjegjësimit për sigurinë kibernetike.

Aktivitetet për realizimin e objektivit do të fokusohen kryesisht në:

- Krijimi i portalit të ndërgjegjësimit me fokus sigurinë kompjuterike, fëmijët në internet, biznesin, këshilla sigurie dhe artikuj.
- Organizimi i fushatave të ndërgjegjësimit në Fakultetet e drejtimit TIK në formën e leksioneve të hapura, seminareve.
- Organizimi i konferencave me sektorin e IT-së mbi prezantimin e udhëzuesit "Për mbrojtjen e të dhënave personale në shërbimet cloud computing"
- Realizimi i aktiviteteve në kuadër të Muajit të ndërgjegjësimit për sigurinë kibernetike
- Krijimi i materialeve informuese (fletëpalosje, broshura, poster)
- Realizimi i aktiviteteve për mbrojtjen e fëmijëve online
- Organizimi i konkurseve me fokus sigurinë për evidentimin e talenteve të reja në fushën e sigurisë kibernetike
- Fushatë ndërgjegjësimi lidhur me sigurinë dhe mbrojtjen kibernetike të rrjeteve kompiuterike me giithë strukturat e FA.

Për realizimin e objektivit, institucionet e përfshira raportuan sa më poshtë:

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) ka raportuar se;

- ✓ Ka krijuar një portal ndërgjegjësimi me fokus sigurinë kompjuterike, fëmijët në internet, biznesin, këshilla sigurie dhe artikuj,
- ✓ Ka krijuar faqen në facebook ¨cyberalbania¨ me objektiv edukimim për një shoqëri dixhitale të sigurtë duke përdorur internet të sigurtë në shtëpi, punë, shkollë etj.
- ✓ ALCIRT dhe AKCE gjatë vitit 2016 kanë organizuar një sërë leksione dhe seminare për çështje të sigurisë kibernetike dhe nënshkrimit elektronik,
- ✓ Ka realizuar aktivitete në kuadër të muajit të ndërgjegjësimit për sigurinë kibernetike,
- ✓ Në muajin Tetor 2016, ALCIRT organizoi konkursin Hack Day Albania duke siguruar një pjesëmarrje të gjerë të të rinjve të talentuar nga Shqipëria dhe Kosova,

- ✓ ALCIRT dhe AKCE kanë organizuar fushata ndërgjegjësimi në Fakultetet e drejtimit TIK në formën e leksioneve të hapura, seminareve.

Komisioneri i të Dhënave Personale (IDP) ka raportuar se;

- ✓ IDP ka publikuar në faqen zyrtare të Zyrës së Komisionerit www.idp.al. Materiale ndërgjegjësuese . ¨Udhëzues për publikimin e fotove të fëmijëve në Internet" dhe "Sugjerime për të mbrojtur privatësinë në internet".
- ✓ Gjithashtu IDP ka organizuar me të rinj të shkollave të mesme shpërndarjen dhe njohjen e materialeve.
- ✓ Ka organizuar konferencave me sektorin e IT-së mbi prezantimin e udhëzuesit "Për mbrojtjen e të dhënave personale në shërbimet cloud computing". Zyra e Komisionerit organizoi më datë më 26/06/2015 workshop-in me temë "Cloud Computing dhe masat e sigurisë për mbrojtjen e të dhënave personale", ku dhe njohu pjesëmarrësit me "Udhëzuesin për Mbrojtjen e të Dhënave Personale në Shërbimet Cloud Computing". Në këtë aktivitet morën pjesë përfaqësues të disa institucioneve, si AKEP e AKSHI, si dhe shumë kompani private që ofrojnë shërbimin Cloud në vendin tonë.
- ✓ Fushatë ndërgjegjësimi "Privatësia dhe siguria e të dhënave gjatë përdorimit të rrjeteve sociale për të rinjtë"

Ministri i Shtetit për Inovacionin dhe Administratën Publike në bashkëpunim me MPB, MAS dhe MMSR në datën 9.02.2016 kanë nënshkruar marrëveshje bashkëpunimi për sigurinë online të fëmijëve në Shqipëri. Objektivat e kësaj Marrëveshjeje janë:

- ✓ Rritja e sigurisë së fëmijëve në Shqipëri gjatë lundrimit të tyre në internet. Krijimi i një mekanizmi kombëtar për identifikimin, raportimin dhe kufizimin e aksesit në faqet me përmbajtje të papërshtatshme për fëmijët në Shqipëri;
- ✓ Forcimin e kuadrit ligjor dhe politikave për sigurinë online të fëmijëve; Krijimi i platformës kombëtare të informacionit, e cila do t'i japë akses fëmijëve, prindërve, mësuesve, grupeve të interesuara, etj, për t'u informuar dhe ndërgjegjësuar mbi sigurinë, rreziqet dhe mënyrat e mbrojtjes nga shfrytëzimi dhe abuzimi online;
- ✓ Shkëmbimin e informacionit në bazë reciprociteti dhe balancimi midis institucioneve, organizatave dhe industrisë së internetit për rritjen e sigurisë në internet të fëmijëve;
- ✓ Forcimi i dialogut midis institucioneve shtetërore, shoqërisë civile, industrisë së internetit dhe komunikimit, për sigurinë në internet, me synim krijimin e një rrjeti komunikimi, bazuar në vullnetin e mirë ndërmjet të gjithë partnerëve që punojnë dhe kujdesen për mbrojtjen online të fëmijëve;
- ✓ Përmbushja e të gjitha angazhimeve të poshtë-përmendura, si pjesë e një qëllimi të përbashkët kombëtar të intensifikimit të përpjekjeve në nivel lokal dhe kombëtar për sigurinë online të fëmijëve;
- ✓ Është lançuar gjithashtu fushata kombëtare mediatike e ndërgjegjësimit e cila po transmetohet në mediat audiovizive dhe billborde.

Autoriteti Kombëtar për Certifikimin Elektronik raportoi se organizoi dhe përfundoi një fushatë ndërgjegjësimi, për përdorimin e identifikimit dhe nënshkrimit elektronik, me qëllim përfitimin e shërbimeve publike online nga qytetarët, të shtrirë në nivel kombëtar.

Drejtoria Arsimore Rajonale/Zyra Arsimore kanë raportuar se në kuadër të këtij objektivi strategjik kanë realizuar aktivitete për mbrojtjen e fëmijëve online;

- ✓ Konferenca Vjetore Kombëtare "Siguria e Fëmijëve në Internet"
- ✓ Fushatë ndërgjegjësuese në 3 DAR për mbrojtjen e fëmijëve online
- ✓ Organizimi i trajnimeve për Sigurinë Kompjuterike për specialistët TIK të DAR/ZA-ve
- ✓ Trajnimi i mësuesve TIK të Drejtorive Rajonale dhe Zyrave Arsimore përkatëse nga personeli TIK i DAR/ZA në sistemin kaskade
- ✓ Krijimi i Posterave Sensibilizues në të gjitha shkollat e DAR/ZA-ve.
- ✓ Përgatitja e broshurës Elektronike dhe e Printuar për DAR/ZA-të.

Ministria e Arsimit dhe Sportit organizoi në vitin 2015 konferencat vjetore kombëtare për Sigurinë e fëmijëve në internet. Ka filluar fushata sensibilizuese në përputhje me planin e veprimit në kuadrin e Marrëveshjes ndërministrore për mbrojtjen e fëmijëve në internet. Si pjesë e angazhimit të mësuesve në programin eTwinning, një pjesë e mësuesve kanë qenë pjesëmarrës të trajnimeve të organizuara në nivel ndërkombëtar për sigurinë e fëmijëve në internet. Me mbështetjen e UNICEF në kuadrin e marrëveshjes ndërministrore janë konceptuar postera sensibilizues në këtë drejtim dhe janë pjesë e fushatës kombëtare.

http://www.arsimi.gov.al/al/newsroom/lajme/nje-kapitull-i-ri-per-sigurine-e-femijeve-ne-internet

http://www.arsimi.gov.al/al/newsroom/lajme/internet-i-sigurt-marreveshje-mes-kater-ministrive

Ministria e Arsimit dhe Sportit në bashkëpunim me Ministrin e Shtetit për Inovacionin dhe Administratën Publike dhe ALCIRT në muajin Maj 2016 në kuadër të javës së inovacionit ALCIRT në bashkëpunim me MSHIAP dhe MAS kanë organizuar aktivitetin ¨Ora e Kodimit¨ pranë shkollës 9 vjeçare ¨Shkolla e Kuqe¨. Ky konkurs me fokus sigurinë, synonte evidentimin e talenteve të reja në fushën e sigurisë kibernetike.

Konkursi “Ora e kodimit” është eventi gjatë Javës së inovacionit 2016 që u kushtohet tërësisht fëmijëve. Në kuadër të nismës ndërkombëtare “Ora e kodimit” të iniciuar në SHBA, MSHIAP, me bashkëpunimin e Ministrisë së Arsimit dhe Sportit, po përfshin në kurrikulën e arsimit 9-vjeçar modulin me zgjedhje “Orët e Kodimit”. Kjo kurrikulë synon të rrisë aftësitë digjitale të nxënësve që në moshë të hershme, me qëllim rritjen e kapaciteteve të tyre në kodim interaktiv.

Shtabi i Përgjithshëm i Forcave të Armatosura ka raportuar fushatë ndërgjegjësimi lidhur me sigurinë dhe mbrojtjen kibernetike të rrjeteve kompjuterike me gjithë strukturat e FA.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), ka raportuar se ka ndërmarrë **f**ushatë ndërgjegjësimi në bashkëpunim me shkolla 9-vjeçare të kryeqytetit, në lidhje me mbrojtjen e fëmijëve nga përdorimi i internetit të pasigurt, në kuadër të ditës ndërkombëtare të internetit të sigurt.

Objektivi 4. Identifikimi dhe mbrojtja e infrastrukturave kritike në Shqipëri

Aktivitetet për realizimin e objektivit do të fokusohen kryesisht në:

- Identifikimi dhe mbrojtja e infrastrukturave kritike dhe infrastrukturave të rëndësishme të informacionit

Për realizimin e objektivit, institucionet e përfshira raportuan sa më poshtë:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), ka raportuar se në kuadër të këtij objektivi, ka identifikuar infrastrukturat kritike dhe të rëndësishme të informacionit dhe ka përgatitur draft VKM për këtë rast

Objektivi 5. Krijimi dhe implementimi i kërkesave minimale të sigurisë

Aktivitetet për realizimin e objektivit do të fokusohen kryesisht në:

- Hartimi e miratimi i kërkesave minimale të sigurisë për administratën
- Numri i certifikatave SSL lëshuar ndaj institucioneve të administratës shtetërore.
- Hartimi e miratimi i masave të sigurisë për bazat e të dhënave shtetëror
- Menaxhimi I përqendruar antivirus.
- Përdorues govnet të cilëve u ofrohet menaxhim i përqendruar antivirusi
- Hartimi e miratimi i kërkesave minimale të sigurisë për administratën
- Hartimi e miratimi i masave të sigurisë për bazat e të dhënave shtetërore

Për realizimin e objektivit, institucionet e përfshira raportuan sa më poshtë:

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) për këtë objektiv ka raportuar se;

- ✓ Ka hartuar kërkesat minimale, gati për tu zbatuar nga administrata publike**.** Udhëzimi për "Masat e sigurisë së Bazave të të Dhënave Shtetërorë" është miratuar me Urdhrin nr.5, datë 12.04.2016.
- ✓ **ALCIRT** dhe **AKSHI** kanë hartuar masat e sigurisë çdo klasë sigurie të bazave të të dhënave shtetërore

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI) raportoi se;

- ✓ Ka rritur numrin e websiteve të administratës te pajisura me certifikate sigurie SSL.
- ✓ Ka rritur numrin e përdoruesve govnet të cilëve u ofrohet menaxhim i përqendruar antivirusi nga AKSHI (8000).
- ✓ Investime në hardware dhe software të automatizuara si masa proaktive dhe reaktive për të siguruar sistemet që administrojnë.
- ✓ Do të rritet siguria në rrjetin qeveritar GovNet dhe qendrën e të dhënave qeveritare.
- ✓ Ngritja e BCC-ve (Business Continuity Center) dhe DRC-ve (Disaster Recovery Center) për rrjetet/sistemet shtetërore
- ✓ Gjatë vitit 2016, AKSHI ka nënshkruar kontratat përkatëse lidhur me ngritjen e BCC-ve (Business Continuity Center) dhe DRC-ve (Disaster Recovery Center) për rrjetet/sistemet shtetërore dhe është në proces implementimi. Aktualisht ka përfunduar faza e lëvrimit, instalimit dhe konfigurimit të infrastrukturës.
- ✓ Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI), gjatë vitit 2016 ka realizuar kontrata përkatësisht për mirëmbajtjen e pajisjeve ekzistuese të sigurisë dhe WAF e-albania.
- ✓ Numri i projekteve TIK të lidhura me sigurinë kibernetike të miratuara nga AKSHI për periudhën 2015-2017 është 23.
- ✓ Përdorues Govnet të cilëve u ofrohet menaxhim i përqendruar antivirusi (10.900)

Drejtoria e Përgjithshme e Policisë së Shtetit ka raportuar për këtë objektiv se;

- ✓ Ka pajisur deri tani me antivirus të licencuar 5000 përdorues dhe është në proces për pajisjen e plotë të gjithë përdoruesve të mbetur me antivirus të licencuar.
- ✓ Policia e Shtetit ka hartuar procedura standarde për të plotësuar kërkesat minimale të sigurisë.
- ✓ Ka hartuar e miratuar masa të sigurisë për bazat e të dhënave shtetërore.

Shtabi i Përgjithshëm i Forcave të Armatosura raportoi se;

- ✓ Në rrjetet kompjuterike të FA është operacional sistemi i qendërzuar Antivirusi për pajisjet fundore.
- ✓ Aplikimi i, Domain Controller, me politikat përkatëse të sigurisë.
- ✓ Fortiguard, mbrojtja e rrjeteve, dedikuar sipas shërbimeve.
- ✓ Aplikimi i ,Firewall, në nyjet kryesore të rrjeteve kompjuterike.

- ✓ Menaxhimi dhe analiza e trafikut në rrjetet kompjuterike të FA (SIEM), Scrutinizer.
- ✓ Sistemi "Backup" i të dhënave për rrjetet kompjuterike të FA.
- ✓ Blerje Pajisje Hardware për Rrjetit NS-WAN për Pikën e Prezencës (PoP) në MM/SHPFA.
- ✓ Implementimi i, Intrusion Prevention System, (IPS).
- ✓ Implementimi i , Intrusion Detection System (IDS).
- ✓ Implementimi i Programeve për skanimin e pikave të dobëta ne rrjet (Vulnerabilities).
- ✓ Zgjerimi i Rrjetit sekret të NATO-s NS-WAN në tre forcat kryesore (FT,FD,FAj).

AKEP për këtë objektiv raportoi se;

- ✓ Gjatë vitit 2015 ka miratuar rregulloren nr.37 datë 29.10.2015 Mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike
- ✓ Gjatë vitit 2017 ka ndërmarrë një sërë inspektimesh pranë sipërmarrësve të komunikimeve elektronike me objekt implementimin e masave teknike dhe organizative për garantimin e sigurisë dhe integritetit të rrjeteve dhe/ose shërbimeve të komunikimeve elektronike.

Drejtoria e Përgjithshme e Tatimeve raportoi për këtë objektiv se;

- ✓ Do të realizohet blerja e System Management Solution (Anti - Malware, controls, mobile security & MDM, Automatic Vulnerability Scanning & patch distribution, protection for Web gatewaz, e-mail & collaboration) dhe Penetration Test,
- ✓ DPT ka parashikuar në PBA 2015-2017 dhe nuk është miratuar fondi për Penetration Test. Është kërkuar blerja e një System Management Solution dhe po për mungesë fondesh nuk është realizuar.
- ✓ Do te merren masa per instalim te sistemeve Microsoft te menaxhimit te (Anti - Malware, controls, mobile security & MDM, Automatic Vulnerability Scanning & patch distribution, protection for Web gateway, e-mail & collaboration) ne bashkepunim me AKSHI.
- ✓ Investime në hardware dhe software të automatizuara si masa proaktive dhe reaktive për të siguruar sistemet që administrojnë.
- ✓ Do të realizohet Upgrade i sistemit checkpoint, Licenca backup,Check point për HA Firewall-in e Internetit, Shërbim penetration testing i sigurisë së rjeteve/sistemeve.

DPT raportoi se për mungesë fondesh, ky objektiv nuk është realizuar.

Shërbimi Informativ i Shtetit raportoi për këtë objektiv se;

- ✓ Ka realizuar investime në hardware dhe software të automatizuara si masa proaktive dhe reaktive për të siguruar sistemet që administrojnë.
- ✓ Ka Ngritur infrastrukturën e sigurisë.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) raportoi se gjatë viteve 2015-2017 numri i incidente kompjuterike të raportuara dhe të trajtuara është 29.

Objektivi 6. Forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit

Aktivitetet për realizimin e objektivit do të fokusohen kryesisht në:

- Pjesëmarrje dhe organizim i aktiviteteve të ndryshme me struktura homologe brenda dhe jashtë vendit

Për realizimin e objektivit, institucionet e përfshira raportuan sa më poshtë:

Shtabi i Përgjithshëm i Forcave të Armatosura për këtë objektiv ka raportuar se;

- ✓ Në stërvitjen e trupave të Ndërlidhjes " Ndërveprimi 2017" për herë të parë u krijua Grupi Teknik për Mbrojtjen Kibernetike. Fokusi i punës së këtij grupi ishte vlerësimi i sigurisë së rrjeteve dhe mbrojtja kibernetike.

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) raportoi se në kuadër të aktiviteteve të ENISA, ALCIRT ka marrë pjesë në aktivitete të ndryshme me partnerët ndërkombëtarë në fushën e sigurisë kibernetike.

ALCIRT, SHPFA, SHISH, DSIK, MPJ, në muajin Nëntor 2016 morën pjesë si lojtarë aktivë në stërvitjen e përvitshme Cyber Coalition Exercise 2016 të organizuar nga NATO.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike raportoi se gjatë vitit 2017 ka organizuar Albanian Cyber Academy 2017 dhe ka marrë pjesë si lojtar aktiv në Cyber Coalition Exercise 2017 (NATO/OTAN), Cyber Czech Exercise 2017.

MSHIAP ka nënshkruar me NATO-n MoU për mbrojtjen kibernetike. Kjo marrëveshje është miratuar më parë në parim nga qeveria e Shqipërisë dhe është e klasifikuar.

Shërbimi Informativ i Shtetit ka realizuar disa marrëveshje me institucione shtetërore të klasifikuara si sekret shtetëror.

Objektivi 7. Rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike

Aktivitetet për realizimin e objektivit do të fokusohen kryesisht në:

- Organizim trajnimesh të ndryshme për stafin si dhe aktivitete sesibilizuese

Për realizimin e objektivit, institucionet e përfshira raportuan sa më poshtë:

ASPA dhe ALCIRT raportojnë se për këtë objektiv kanë organizuar dhe kryer trajnime për profesionistët IT të administratës publike me modulin bazë dhe të avancuar të sigurisë kibernetike.

Policia e Shtetit gjatë viteve 2016 dhe 2017 ka organizuar trajnime për profesionistët IT të administratës së saje në modulin bazë dhe të avancuar të sigurisë kibernetike.

Banka e Shqipërisë ka organizuar për të gjithë punonjësit e saj trajnim/edukim mbi sigurinë informatike për të gjithë punonjësit e Bankës së Shqipërisë me fokus ndërgjegjësimin mbi rreziqet kibernetike, njohjen me teknikat e përdorura nga sulmuesit kibernetikë, si dhe mënyrën e mbrojtjes ndaj këtyre sulmeve me qëllim zvogëlimin e rreziqeve.

KDIMDP gjatë viteve 2015-2016-2017 ka organizuar Workshop Konference me sektorin IT mbi prezantimin e udhëzuesit për mbrojtjen e të dhënave personale në shërbimet Ecloud si dhe fushata ndërgjegjësimi "Privatësia dhe siguria e të dhënave gjatë përdorimit të rrjeteve sociale për të rinjtë".

IZHA raportoi se ka përfshirë në kurikula të çështjeve të sigurisë kibernetike në arsimin para universitar për një internet më të sigurtë. Gjithashtu angazhohet se do të integrohet TIK në kurikulën e arsimit para universitar.

- ✓ Për vitin 2015-2016, ka realizuar programe shkollore për mësuesit për klasat e 6-ta, 7-ta. Për klasat e 8-ta planifikohet të kryhen në vitin 2017. Trajnimi i mësuesve të klasave të 6-ta dhe të 7-ta për kurrikulën e re të TIK-ut.
- ✓ Gjithashtu hartimi i broshurës elektronike për mbrojtjen kibernetike për mësuesit e arsimit 9-vjecar dhe mësuesit e arsimit të mesëm të lartë është parashikuar për tu realizuar .

Universiteti i Tiranës raportoi se ka realizuar **s**tudime pasuniversitare (dega master) të specializuara drejt sigurisë kibernetike duke krijuar programin master për siguri informacioni pranë fakultetit të ekonomisë, dega informatikë ekonomike.

ALCIRT dhe **AKCE** janë bashkuar si një institucion në varësi të Këshillit të Ministrave Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)duke mundësuar ndryshimin e strukturave dhe shtimin me specialistë të fushës së sigurisë.

Drejtoria e Përgjithshme e Dogana angazhohet për rritjen e kapaciteteve për stafin përgjegjës të DPD.

Shtabi i Përgjithshëm i Forcave të Armatosura raportoi se për këtë objektiv se;

- ✓ Me personelin planifikues dhe atë menaxhues të SNI të FA janë organizuar, seminare dhe takime , për njohjen me dokumentin, si dhe kërkesat e detyrimet që rrjedhin.
- ✓ Me personelin e emëruar rishtazi në Forcat e Armatosura zhvillohen trajnime të shkurtra për përdorimin e sistemeve të komunikimit dhe të informacionit dhe sigurinë e tyre.
- ✓ Gjatë periudhës 2015-2017, personeli i strukturave të FA ekspertë të fushës kibernetike, është trajnuar në shkollat e NATO-s.
- ✓ Në kuadër të planit të bashkëpunimit dy palësh midis Ministrisë së Mbrojtjes dhe Shteteve të Bashkuara te Amerikës, ekspertë të Gradës Kombëtare të New Jersey, gjatë periudhës 2013-2017, kanë zhvilluar trajnim 1 (një) javor lidhur me çështje të sigurisë kibernetike dhe mbrojtjen e rrjeteve kompjuterike "Cyber Security Program". Në këtë trajnim kanë marrë pjesë ekspertë të fushës nga FA, MM, DSIK, SHISH dhe ALCIRT. Gjithashtu ekspert të fushës i FA kanë marrë pjesë në seminare, workshope dhe aktivitete për çështje të sigurisë së rrjeteve kompjuterike dhe mbrojtjen kibernetike.
- ✓ Në kuadër të promovimit të bashkëpunimit në nivel rajonal për çështje të mbrojtjes kibernetike, është marrë pjesën në workshope, seminare dhe aktivitete rajonale të zhvilluara për këtë qëllim ku mund të përmendim dy workshope rajonale të zhvilluara Slloveni dhe Kroaci "Balkans Regional Cyber Defense Workshop".

IV. PËRFUNDIME

Ky dokument politikash si dokumenti i parë strategjik i këtij lloji, synon tërheqjen e vëmendjes si dhe identifikimin e problematikave dhe të zgjidhjeve për çështjet e sigurisë kibernetike.

Mbështetja e Qeverisë si dhe e institucioneve të varësisë nëpërmjet iniciativa të ndryshme, kanë krijuar një mjedis dixhital më të sigurtë. Miratimi i ligjit për "Sigurinë Kibernetike" konsiderohet si treguesi më i lartë i mbështetjes në nivel politik.

Nga analizimi i bërë situatës, gjatë raportimit përfundimtar, vlerësojmë se për të pasur një mjedis dixhital sa më të sigurtë duke aplikuar masat e duhura për të menaxhuar rreziqet e sigurisë, del si sfidë e jona në vazhdimësi, trajnimi i personave të dedikuar si dhe duhet të ndërmerren investime të mëtejshme.

Aktorët e angazhuar në këtë dokument politikash kanë realizuar objektivat e marr përsipër, me përjashtim të rasteve kur për shkak të specifikave të veçanta, ato janë në proces realizimi.

Siç shihet edhe nga ky raport, kemi një përpjekje pozitive bazuar në angazhimet e mara por edhe në plane të reja të cilat kanë çuar në hapa përpara çështjet e sigurisë kibernetike. Gjithsesi duhet të ngulmohet për një qasje të drejtë në këto çështje nga të gjithë aktorët e përfshirë.

Duke analizuar situatën dhe konsideruar zhvillimet e shpejta teknologjike që po ndodhin në botë, të cilat sjellin ndikimet e tyre edhe në Shqipëri, është e domosdoshme që të kalohet në një nivel më të lartë politikash duke përcaktuar një Strategji Kombëtare për Sigurinë Kibernetike.

Hartimi i Strategjisë Kombëtare për Sigurinë Kibernetike do ta rendisë Shqipërinë krah vendeve të tjera të NATO-s, duke treguar koordinim e bashkëpunim me të gjithë aktorët e fushës, me qëllim rritjen e nivelit të sigurisë së hapësirës kibernetike.

.