Republika e Kosovës
Republika Kosova - Republic of Kosovo
Qeveria – Vlada - Government
Ministria e Mbrojtjes
Ministarstvo Odbrane Ministry of Defense
Drejtoria e Mbështetjes/Direktorij Podrška/Support Directory
Departamenti i KTI-së/ Departament za Veze i Informatiku/ CIT Department

LISTË DISTRIBUIMI/ CIRKULARNO PISMO/ ROUTING SLIP

REFERENCË:		6/2/48/2024			
PËR/ZA/TO:		z. Ejup MAQEDONCI Ministër i Mbrojtjes			
CC:		z. Zijadin BAJQINCA Drejtor i Drejtorisë së Mbështetjes			
PËRMES/PREKO/THROUGH:		z. Gafurr DUGOLLI U.d. Sekretar i përgjithshëm i MM-së			
NGA/OD/FROM:		z. Beqir BYTYQI Drejtor i Departamentit të KTI-së			
TEMA/SUBJEKAT/SUBJECT:		Kërkesë			
Nr. i zyrës: **Br. kancelarije:** **RoomNo.:**	**34**	**Lokacioni:** **Kucni:** **Extension:**	**MM**	**Data:** **Datum:** **Date:**	07.06.2024
PËR AKTIVITET/ZA AKTIVNOST/FOR ACTION					☐
PËR MIRATIM/ZA USVAJANJE/FOR APPROVAL					☒
PËR NËNSHKRIM/ZA POTPIS/FOR SIGNATURE					☒
PËR KOMENTE/ZA KOMENTARE/FOR COMMENTS					☐
A MUND TË DISKUTOJMË/DALI MOZEMO RASPRAVLJATI/MAY WE DISCUSS					☐
VËMENDJA JUAJ/VASA PAZNJA/YOUR ATTENTION					☐
SIPAS DISKUTIMIT/KAKOJE RASPRAVLJENO/AS DISCUSSED					☐
SIÇ ËSHTË KËRKUAR/KAKO JE ZATRAZENO/AS REQUESTED					☐
SHËNIM DHE PËRGJIGJE/BELESKA I ODGOVOR/NOTE AND RETURN					☐
PËR INFORMIMIN TUAJ/ZA VASU INFORMACIJU/FOR YOUR INFORMATION					☐
AFATI/KRAJNI ROK/DEADLINE					

Të nderuar,

Bashkangjitur kërkesën për miratimin e Strategjisë për Mbrojtje Kibernetike 2024-2028.

Me respekt,

Adresa: Kazerma "Adem Jashari" -10 000 Prishtinë-Kosovë
Telefon/Faks: + 38344 159 287 /038 200 13 575
https://www.mod.rks-gov.net, E-mail: beqir.bytyqi@rks-gov.net

Republika e Kosovës

Republika Kosova - Republic of Kosovo

Qeveria – Vlada - Government

Ministria e Mbrojtjes

Ministarstvo Odbrane Ministry of Defense

Drejtoria e mbështetjes /Direktorat za podršku/Directorate for Support

Departamenti i KTI-së/ Departament za Veze i Informatiku/ CIT Department

---

Strategjia për Mbrojtje Kibernetike në MM/FSK 2024-2028

Miratoi:

Ejup MAQEDONCI

Ministër i Mbrojtjes

Qershor 2024

REFERENCAT

- Ligji nr. 06/L-122 për Ministrinë e Mbrojtjes[1];
- Ligji nr. 06/L-123 për Forcën e Sigurisë së Kosovës[2];
- Ligji nr. 08/L-173 për sigurinë kibernetike[3];
- Ligj nr. 06/L-014 për Infrastrukturën Kritike[4];
- Strategjia Kombëtare për Sigurinë Kibernetike 2023-2027[5]
- Strategjia e Mbrojtjes e Republikës së Kosovës;
- Ligji nr. 03/L-050 për Themelimin e Këshillit të Sigurisë së Kosovës[6];
- Ligji nr. 04/L-109 për Komunikimet Elektronike[7];
- Ligji nr.06/L – 082 për Mbrojtjen e të Dhënave Personale[8];
- Ligji nr. 04/L-052 për Marrëveshjet Ndërkombëtare[9];
- Ligji nr.08/L-175 për mbrojtjen e informacionit të klasifikuar[10];
- Analiza e rishikimit strategjik të sektorit të sigurisë në Republikën e Kosovës;

---

[1] https://gzk.rks-gov.net/ActDetail.aspx?ActID=18374

[2] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2523

[3] https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933

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

[5] https://mpb.rks-gov.net/Uploads/Documents/Pdf/AL/2692/Strategjia%20p%C3%ABr%20Siguri%20Kibernetike%20-%20ALB..pdf

[6] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2521

[7] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851

[8] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2676

[9] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2789

[10] https://gzk.rks-gov.net/ActDetail.aspx?ActID=71104

PËRMBAJTJA

I. LISTA E SHKURTESAVE DHE PËRKUFIZIMI I TERMAVE

Në këtë paragraf do të paraqiten shkurtesat dhe definicionet e termave specifikë të përafruar me kuptimin themelor të këtyre termave në vendet e BE-së dhe NATO-së.

Shkurtesat

CERT	Ekipi Reagues për Emergjenca Kompjuterike
CSIRT	Ekipi Reagues për Incidentet e Sigurisë Kompjuterike
DKTI	Departamenti i Komunikimit dhe TI-së
ENISA	Agjencia Evropiane për Sigurinë e Rrjeteve dhe Informacionit
FSK	Forca e Sigurisë së Kosovës
GK	Garda Kombëtare
IKI	Infrastruktura Kritike e Informacionit
SHP	Shtabi i Përgjithshëm
NJMK	Njësia për Mbrojtje Kibernetike
NJK	Njësia e Komunikimit
MM	Ministria e Mbrojtjes
TIK	Teknologjia e informacionit dhe Komunikimit
SIEM	Security Information and Event Monitoring
OShE	Operatorët e Shërbimeve Esenciale
OShD	Ofruesit e Shërbimit Digjital.

Përkufizimi i termave

Kibernetika nënkupton mjedis kompleks që lind nga ndërveprimi i njerëzve, programeve kompjuterike dhe shërbimeve në hapësirën kibernetike, me anë të pajisjeve të rrjeteve teknologjike që lidhen në të, që nuk ekziston në formë fizike.

Hapësira kibernetike është mjedisi digjital i aftë të krijojë, të procesojë dhe të shkëmbejë informacionin e krijuar nga sistemet, shërbimet e shoqërisë së informacionit, si dhe rrjetet e komunikimit elektronik.

Siguria kibernetike nënkupton aktivitetet e nevojshme për të mbrojtur sistemet e rrjetit dhe informacionit, përdoruesit e këtyre sistemeve dhe personave të tjerë të prekur nga kërcënimet në internet.

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

Sulmi kibernetik është sulm në sistemin e TIK në hapësirën kibernetike, i drejtuar ndaj një apo më shumë sistemeve teknologjike, me qëllim të cenimit të sigurisë së TIK-ut.

Spiunim kibernetik quhen sulmet kibernetike kundër konfidencialitetit të një sistemi TIK-ut, të cilat ushtrohen apo menaxhohen nga shërbimet e huaja inteligjente.

Sabotim kibernetik quhen sulmet kibernetike ndaj integritetit dhe disponueshmërisë së sistemeve të TIK-ut.

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

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

Infrastruktura kritike e informacionit (IKI) nënkupton sistemet TIK-ut që janë infrastruktura kritike për vetveten apo që janë thelbësore për funksionimin e infrastrukturave kritike (telekomunikacioni, kompjuterët/softuerët, Interneti, satelitët etj.).

Operatori i shërbimeve esenciale është entitet që i plotëson kriteret në vijim:

- Entiteti që ofron një shërbim i cili është esencial për mirëmbajtjen e aktiviteteve kritike shoqërore dhe/ose ekonomike,
- Ofrimi i atij shërbimi varet nga rrjeti dhe sistemet e informacionit, dhe
- Një incident do të kishte efekte të rëndësishme në ofrimin e atij shërbimi.

Ofruesi i shërbimit digjital çdo person juridik që ofron një shërbim digjital.

Ekipi reagues ndaj emergjencave kompjuterike (CERT) apo shkurtimisht CERT është përgjegjëse për pranimin, shqyrtimin dhe reagimin ndaj incidenteve dhe aktiviteteve të tjera kundër sigurisë kompjuterike. Emërtime të tjera për grupe të tilla mund të jenë ekipet e gatishmërisë për emergjenca kompjuterike dhe ekipe reaguese ndaj incidenteve të sigurisë kompjuterike (CSIRT).

Cyber Range është një laborator ose mjedis simulimi i sulmeve kibernetike që përdoret për të zhvilluar ushtrime, trajnime dhe testim të politikave dhe procedurave të sigurisë duke ndihmuar institucionet të përmirësojnë reagimin ndaj sulmeve kibernetike.

Ushtrime në fushën e sigurisë kibernetike janë aktivitete të simuluara për të testuar përgjigjen dhe qëndrueshmërinë e institucioneve ndaj sulmeve kibernetike, që shërbejnë në identifikimin e dobësive dhe përmirësimin e masave të sigurisë në sistemin e TI-së.

II. PËRMBLEDHJE EKZEKUTIVE

Sot jemi duke jetuar në një botë të zhvillimit dhe avancimit të shpejtë të teknologjisë informative dhe përdorimit të tyre në çdo lëmi të jetës. Kur flasim për pajisjet e teknologjinë informative assesi nuk mund të lëmë anash kyçjen e tyre në internet.

Penetrimi i Internetit në Kosovë është në shkallë të ngjashme me mesataren e Bashkimit Evropian (BE), derisa edhe sjelljet e qytetarëve të Kosovës në Internet duket të jenë të ngjashme me trendët globale.

Me përdorimin e madh të Internetit si platformë kryesore e punës, shkencës dhe komunikimit social të qytetarit modern, siguria dhe privatësia e tij kthehen në brenga kryesore. Që nga fillimi i vitit 2020, me situatën e krijuar nga pandemia COVID-19 ku shumë institucione dhe organizata kanë punuar nga shtëpia ka bërë që një praktikë e tillë të vazhdojë edhe në ditët e sotme. Kjo praktikë e punës nga distanca ka krijuar një ambient mjaft të favorshëm për keqbërësit në internet të cilët munden më lehtë të kryejnë veprimet e tyre keqbërëse (vjedhje, manipulime, shantazhe, mashtrime etj.). Organizata ndërkombëtare policore Interpol, ka paralajmëruar për shkallën alarmante të krimeve kibernetike gjatë pandemisë, kur kriminelët duket se e kanë shfrytëzuar kohën kur shumë njerëz po punojnë nga shtëpia për të vënë në shënjestër institucione të rëndësishme. Sipas një vlerësimi të kësaj organizate me seli në Francë, është vërejtur një ndërrim i ndjeshëm i shënjestrave të kriminelëve kibernetik nga individët dhe bizneset e vogla te korporatat e mëdha, qeveritë dhe infrastruktura kritike.

Të gjitha institucionet shtetërore dhe ato private funksionimin e tyre për çdo gjë e kanë të lidhur ngushtë me hapësirën kibernetike që nga transaksionet financiare e deri të çështjet ushtarake.

Edhe Ministria e Mbrojtjes dhe Forca e Sigurisë së Kosovës (tutje MM/FSK) si shumë institucione tjera të Kosovës një numër të madh të punëve ditore i kryen në sistemin që ka qasje në internet dhe me këtë është rritur edhe shkalla e mundësisë së keqpërdorimit apo edhe humbjes së informacioneve nga përdoruesit për qëllime të caktuara dashakeqëse e që janë pjesë e internetit. Sipas "Analizës së rishikimit strategjik të sektorit të sigurisë në Republikën e Kosovës", krimi kibernetikë është identifikuar si një prej rreziqeve, sfidave apo kërcënimeve globale që mund të cenojnë edhe sigurinë e Kosovës.

Strategjia e Mbrojtjes e Republikës së Kosovës po ashtu identifikon sulmet kibernetike si njërin nga sfidat dhe rreziqet aktuale që i kanosen vendit tonë. Në Strategjinë e Mbrojtjes së Republikës së Kosovës theksohet se "*mjedisi i sigurisë vazhdon të mbetet i paqëndrueshëm, i pasigurt, kompleks dhe i paqartë*", dhe se "*Republika e Kosovës, me gjithë zhvillimet pozitive, kërcënohet, rrezikohet dhe sfidohet nga: qasja armiqësore e Serbisë, ndërhyrjet e jashtme, sulmet kibernetike, ekstremizmi nacional dhe fetar, fatkeqësitë natyrore dhe fatkeqësitë e tjera*".

Pra të gjitha informacionet që janë ose transmetohen përmes internetit në të njëjtën kohë i ekspozohen edhe rreziqeve të ndryshme të natyrës kibernetike përmes aktorëve shtetëror apo jo shtetëror. Këto rreziqe apo siç njihen ndryshe sulmet kibernetike mund të shkaktojnë dëme të pa riparueshme për MM dhe FSK duke shkaktuar humbjen e informacioneve, dëmtimin e shkëmbimit të informacioneve, pengimin e punës normale, sabotazha, dëmtimin e imazhit etj.

III. HYRJE

MM dhe FSK ka një numër të madh të pajisjeve digjitale të TIK e që përmes tyre zhvillohen aktivitetet e ndryshme të punës së tyre. Për këtë arsye duhet t'i kushtohet rëndësi e veçantë fushës së sigurisë kibernetike në MM/FSK duke ndjekur praktikat dhe standardet me të cilat operojnë edhe vendet e NATO-s.
Në korrik të vitit 2016 në Samitin e Varshavës vendet anëtare të NATO-së kanë ri-konfirmuar mandatin mbrojtës që NATO kishte aktualisht, si dhe njëkohësisht kanë njohur hapësirën kibernetike si fushë e pestë operacionale ushtarake; "*NATO mbron hapësirën e saj kibernetike në mënyrë efektive sikurse mbron veten e saj në ajër, në tokë dhe në det*".
Me ndryshimin e misionit dhe përgjegjësive të MM/FSK, kanë dalë detyra dhe përgjegjësi shtesë për çështjet e sigurisë në vend lidhur me mbrojtjen e territorit të RKS duke përfshirë edhe përgjegjësitë për mbrojtjen e hapësirës kibernetike.

Përdorimi i teknologjisë informative dhe komunikimit mundëson MM/FSK-së të kenë efikasitet më të madh në komandim – kontroll, mbështetje logjistike dhe në të gjitha shërbimet tjetra të cilat mbështetën në sistemin e TIK-ut. Duke pasur parasysh sot në botë trendët e globalizimit që janë të ndërlidhura me hapësirën e sigurisë kibernetike, e bënë që siguria kibernetike të jetë një nga objektivat kyçe strategjike të sigurisë në MM/FSK dhe po ashtu në tërë vendin. Disa nga detyrat kryesore në fushën e mbrojtjes kibernetike është mbrojtja e sistemeve, rrjeteve dhe informacionet në MM/FSK, bashkëpunimi me agjencitë tjera shtetërore për të kontribuar në minimizimin dhe parandalimin e sulmeve kibernetike në nivel vendi si dhe MM/FSK të jetë në gjendje që të kryej me sukses operacione në fushën e mbrojtjes kibernetike. MM/FSK mbështetet në përdorimin e rrjeteve të sigurta për ruajtjen apo shkëmbimin e informacioneve me qëllim të përmbushjes së misionit dhe realizimin e detyrave të veta sipas këtij misioni. Duke pasur parasysh trendët e sotme të zhvillimit të teknologjisë së informacionit dhe nivelin e lartë të njohurive për këtë fushë MM/FSK duhet të kenë kujdes të madh dhe t'i kushtojnë rëndësi të veçantë mbrojtjes së sistemeve të tyre nga sulmet e mundshme kibernetike.

MM/FSK synon të ketë sisteme dhe rrjete elektronike të operueshme, të qëndrueshme dhe të besueshme, sisteme këto që do të mbështesin komunikimin e sigurt brenda dhe jashtë institucionit të MM/FSK si dhe vendosjen e standardeve për të operuar në hapësirë të sigurt kibernetike.

IV. QËLLIMI

Qëllimi i këtij dokumenti është vendosja e objektivave të MM/FSK në fushën e sigurisë kibernetike dhe përcaktimi i aktiviteteve mbështetëse për realizimin e objektivave në funksion të ngritjes dhe zhvillimit të kapaciteteve të sigurisë kibernetike për pesë vitet vijuese (2024-2028).

V. VIZIONI

Vizioni i Strategjisë së mbrojtjes kibernetike është të krijojë dhe të mbajë një mjedis digjital të sigurt dhe të qëndrueshëm në MM/FSK, nëpërmjet ngritjes së kapaciteteve profesionale, rritjes së vetëdijes për rreziqet dhe kërcënimet, si dhe ndërtimit të besimit dhe forcimit të bashkëpunimit vendor dhe ndërkombëtar në fushën e sigurisë kibernetike.

VI. PARIMET E PËRGJITHSHME

Strategjia për Mbrojtje Kibernetike në MM/FSK do të trajtoj hapësirën kibernetike si një fushë operacionale me qëllim të organizimit, zhvillimit të aftësive dhe zhvillimit të kapaciteteve ashtu që MM/FSK të mund të veprojë në mbrojtjen e sistemeve të teknologjisë informative dhe komunikimit.

Ministria e Mbrojtjes në harmoni me bazën ligjore për siguri kibernetike në nivel vendi, si dhe duke respektuar të gjitha parimet që rrjedhin nga marrëveshjet ndërkombëtare dhe iniciativat tjera që do të ndërmerren në këtë fushë, synon që të krijoj mekanizma në funksion të mbrojtjes së konfidencialitetit, integritetit dhe disponueshmërisë së informacionit të MM/FSK si dhe të jetë gatshme të ndihmojë institucionet e qeveritare, OShE dhe OShD në raste të emergjencave kibernetike.

Strategjia për mbrojtje kibernetike do të adresoj këto çështje:

- Adresimin e kërcënimeve që për fokus e kanë dëmtimin e sistemeve të TIK në MM/FSK
- Vetëdijesimin e personelit për rreziqet ndaj sulmeve kibernetike
- Ngritjen e njohurive specialistike në fushën e sigurisë kibernetike
- Ndërtimin e besueshmërisë mbi sigurinë e përdorimit të sistemeve të TIK në MM/FSK
- Bashkëpunimin dhe shkëmbimin e informacionit në fushën e sigurisë kibernetike me institucionet vendore të sigurisë dhe partnerët ndërkombëtar të MM/FSK-së.

MM/FSK ka përcaktuar pesë objektivat strategjike në funksion të kryerjes së misionit në fushën e sigurisë kibernetike:

1. Zhvillimi i kapaciteteve ushtarake për të kryer operacione kibernetike
2. Ngritja e vetëdijes dhe forcimi i njohurive në fushën e sigurisë kibernetike brenda MM/FSK duke përfshirë rekrutimin dhe mbajtjen e personelit të kualifikuar
3. Ngritja dhe funksionalizimi i Qendrës Shtetërore Trajnuese për Siguri Kibernetike
4. Identifikimi dhe mbrojtja e infrastrukturës kritike të informacionit në MM/FSK
5. Intensifikimi i bashkëpunimit kombëtar dhe ndërkombëtar

VII. SFIDAT E SIGURISË

Sfidat e sigurisë për Sistemet e TIK përfshijnë të gjitha nivelet e strukturave të MM/FSK-së duke filluar nga pajisjet zyrtare personale të punës, deri në sigurimin e sistemeve themelore, të cilat janë kritike për mbarëvajtjen e punës. Disa nga sfidat që karakterizojnë këtë situatë dhe orientimi i tyre për të ardhmen përfshinë:

1. Ndërgjegjësim i ulët për rreziqet në fushën e sigurinë kibernetike dhe mungesa e sistemit të menaxhimit të rrezikut

"Hallka më e dobët në zingjirin e sigurisë së një sistemi të TIK-ut janë njerëzit, jo Teknologjia". Edhe institucionet me standardet më të larta të sigurisë, janë të prirur ndaj gabimeve njerëzore. Kjo për shkak se njerëzit janë pjesa më e rëndësishme e sigurisë së informacionit dhe të gjithë njerëzit bëjnë gabime.
Ndërsa ne e dimë se gabimet njerëzore janë arsyeja kryesore për mbi gjysmën e të gjitha shkeljeve të sigurisë në sistemin e TIK-ut, shumica e tyre janë pa qëllim.
Krejt çka i nevojitet një sulmuesi është një derë e hapur në rrjetin e institucionit tuaj. Nëse kjo arrihet nga gabimi njerëzor, atëherë masat e sigurisë të zbatuara për të mbrojtur të dhënat tuaja nuk janë të dobishme. Disa arsye kryesore për dobësitë njerëzore janë:

- Mungesa e njohurive për sigurinë.
- Mosnxënia e hapit me zhvillimet e reja teknologjike dhe kërcënimet që ndërlidhen me to.
- Pakujdesia.
- Mosrespektimi i politikave dhe procedurave.

Sistemi i menaxhimit të rrezikut është mjaft kompleks dhe vështirë i realizueshëm i cili kërkon staf të trajnuar mirë në të gjitha nivelet për të kuptuar dhe vlerësuar drejt kërcënimet dhe rreziqet e mundshme për institucionin. Për këtë arsye, ka mungesë të një sistemi të tillë në të gjitha institucionet e vendit dhe po ashtu edhe në institucionin tonë.

2. Mungesa e specialistëve në fushën e sigurisë kibernetike si dhe mungesa e politikave për rekrutimin, zhvillimin dhe mbajtjen e talenteve të ri

Krimet kibernetike janë në zhvillim të vazhdueshëm sa i përket llojllojshmërisë dhe shpejtësisë se tyre dhe mungesa e specialistëve në fushën e sigurisë kibernetike është mjaft sfiduese për sektorin e sigurisë në vend dhe jo vetëm. Kjo për arsye se përgatitja e një specialisti në këtë fushë kërkon kohë dhe mjete financiare për mbajtjen e trajnimeve të nevojshme për të qenë në hap me zhvillimin e hovshëm të teknologjisë. Me arritjen e një niveli të kënaqshëm të specializimit në këtë fushë, këta persona janë mjaft të kërkuar nga tregu. Kompanitë private vendore dhe ndërkombëtare ofrojnë mundësi të mira punësimi për specialistët e sigurisë kibernetike dhe TIK në përgjithësi, gjë që e vështirëson mbajtjen e tyre brenda institucionit.

3. Përdorimi i madh i internetit dhe pajisjeve mobile

Përdorimi gjithnjë e në rritje i internetit dhe i sistemeve të reja kompjuterike, telefonave mobil dhe pajisje tjera teknologjike e bëjnë të mundshme rritjen e efikasitetit të punës por në anën tjetër vështirësojnë mbrojtjen e të dhënave dhe paraqesin kërcenim për sigurinë e sistemit të TIK-ut në MM/FSK.

4. Inteligjenca artificiale

Zhvillimi i inteligjencës artificiale sjell shqetësime të mëdha për sigurinë kibernetike. Inteligjenca artificiale përveç dobive në fushën e sigurisë kibernetike me vete mbartë edhe rreziqe të shumta, duke pasur parasysh se për një kohë relativisht të shkurtër iu mundëson keqbërësve krijimin e sulmeve të avancuara ndaj sistemeve të informacionit dhe infrastrukturave kritike në përgjithësi. Duke pasur parasysh që është një vegël aq e fuqishme, rreziku i përdorimit të vetive pozitive për qëllime të këqija të individëve, grupeve ose organizatave të caktuara është shumë i madh.

5. Kërcënimet dhe rreziqet në hapësirën kibernetike

Duke pasur parasysh trendët e shpejta të zhvillimit të teknologjisë si dhe përhapjen e grupeve terroriste në botë bënë që sulmet kibernetike të jenë një nga kërcënimet kryesore strategjike në nivel vendi. Edhe pse ne si vend ende nuk e kemi një zhvillim ekonomik të mirë si dhe jemi në fazën e tranzicionit në forcë të armatosur, prapëseprapë ekziston rreziku nga kërcënimet e mundshme përmes sulmeve të hapësirës kibernetike qoftë nga akterët shtetëror apo jo shtetëror me qëllim të prishjes së imazhit Kosovës në rajon dhe botë.

6. Kërcënimet nga spiunazhi dhe sabotazha

Me zhvillimin e procesit të transformimit të MM dhe FSK-së, institucioni ynë do të jetë gjithnjë e më shumë pikësynim i sulmeve kibernetike dhe për këtë arsye spiunazhi dhe sabotazhi na bëjnë më të ndjeshëm për të rënë pre synimit të tyre ndaj sistemeve të TIK.

7. Besueshmëria e vetë punonjësve

Keqpërdorimi, humbja dhe vjedhja e informacionit nga vetë punonjësit e MM\FSK-së paraqet një dukuri të vështirë për tu zbuluar.

8. Përhapja e programeve të dëmshme (Malware)

Përhapja në nivel global e programeve dhe softuerëve të dëmshëm ("malware") e rritë rrezikun e kërcënimeve ndaj të dhënave dhe rrjeteve të RKS, po ashtu këto rreziqe mund të shfaqen edhe ndaj rrjeteve dhe informacioneve të FSK-së.

9. Rreziqet e infrastrukturës kritike dhe rrjeteve të MM/FSK

Sistemet dhe rrjetet e MM-së dhe FSK-së janë të ekspozuara ndaj cenueshmerisë nga ndërhyrjet dhe sulmet. Përveç sulmeve të infrastrukturës kritike të MM/FSK, një sulm kibernetik ndaj infrastrukturës kritike ose burimeve kyçe në nivel shteti, ku MM/FSK ka një lidhshmëri apo shfrytëzon disa nga këto burime në kryerjen e operacioneve të veta, mund të ndikojnë në aftësitë e FSK-së për të operuar.

10. Mbajtja e mjedisit të sigurt në të ardhmen

Duke pasur parasysh kërcënimet e ditëve të sotme, MM duhet të kontribuojë në zhvillimin dhe zbatimin e një strategjie gjithëpërfshirëse për mbrojtje kibernetike për të parandaluar dhe penguar akterët e ndryshëm në kryerjen e sulmeve kibernetike kundër interesave të MM/FSK.

11. Privatësia dhe identiteti

Privatësia personale është gjithashtu e ekspozuar ndaj rreziqeve të sulmeve kibernetike për shkak të metodave të reja të komunikimit dhe mënyrave të përdorimit të sistemeve të informacionit dhe internetit.
Abuzimi me identitetin është një sfidë në rritje për çdo individ dhe autoritet institucional.

12. Kufizimet financiare

Kufizimet financiare janë një sfidë tjetër që ndikojnë në ngritjen e kapaciteteve për siguri kibernetike. Duke konsideruar që mbrojtja kibernetike për shumë vende dhe institucione është ndër fushat më me prioritet, investimet në "mbrojtjen kibernetike" janë të nevojshme të jenë në nivelin që i korrespondon me mbrojtjen ndaj rreziqeve aktuale.

VIII. OBJEKTIVAT STRATEGJIKE

Bazuar në sfidat e sigurisë në fushën e mbrojtjes kibernetike, MM/FSK ka identifikuar pesë objektiva strategjike për zhvillimin dhe ngritjen e kapaciteteve për siguri kibernetike për 5 vitet e ardhshme. Strukturat e MM dhe FSK si dhe i gjithë personeli duhet të përfshihen në mbrojtjen e sigurisë të sistemeve të TIK-ut në mënyrë sistematike.

1. ZHVILLIMI I KAPACITETEVE USHTARAKE PËR TË KRYER OPERACIONE KIBERNETIKE

Strategjia e mbrojtjes kibernetike përmes këtij objektivi strategjik synon ngritjen e kapaciteteve dhe aftësive ushtarake për të kryer operacione kibernetike gjatë pesë viteve të ardhshme.

Për zhvillimin dhe avancimin e këtyre aftësive duhet të hartohet dokumentacioni i nevojshëm, plotësimi me personel, realizimi i trajnimeve specialistike, ngritja e qendrës për operacione të sigurisë kibernetike dhe funksionalizimi i veglave të nevojshme për kryerjen e aktiviteteve për secilën aftësi.

Hartimi i dokumentacionit në fushën e sigurisë kibernetike është esencial për mbrojtjen e infrastrukturës së informacionit dhe të dhënave. Ky dokumentacion duhet të përfshijë kriteret bazë deri te ato më të avancuara të sigurisë kibernetike që duhet të implementohen në sistemin e TIK-ut. Në hartimin e dokumentacionit përfshihen:

- **Politikat** e sigurisë për rrjetet e komunikimit dhe informacionit me të cilat rregullohen parimet dhe standardet e përgjithshme për kontrollet kritike të sigurisë.
- **Udhëzuesit** e sigurisë së konfigurimeve në rrjet të cilat obligojnë administratorët e serverëve dhe rrjetit të bëjnë konfigurimet sipas këtyre udhëzuesve.

Është esenciale të plotësohen pozitat e planifikuara në strukturat përgjegjëse për siguri kibernetike në MM dhe FSK. Plotësimi me kapacitetet e duhura njerëzore i strukturës për mbrojtje kibernetike duhet të përfundojë në trevjetorin e ardhshëm deri në ngritjen e kapaciteteve të plota.

Përveç stafit profesional, MM/FSK duhet të ketë në dispozicion edhe pajisjet dhe veglat teknike që për të kryer detyrat e përcaktuara në mbrojtjen e hapësirës kibernetike në MM\FSK.

Përmbushja e objektivit 1 strategjik synohet të arrihet përmes 4 objektivave specifike:

1.1 Ngritja e Qendrës për Operacione të Sigurisë (SOC – Security Operation Center)

Qendra për Operacione të Sigurisë do të shërbejë për monitorimin e vazhdueshëm të sistemeve të TIK-ut për të identifikuar/zbuluar rreziqet dhe kërcënimet kibernetike me qëllim të parandalimit dhe mënjanimit së sulmeve kibernetike. Monitorimi bëhet nga ekipe brenda Njësisë për mbrojtje kibernetike në SHP. Ky monitorim nënkupton mbikëqyrjen e vazhdueshme të ngjarjeve jo të zakonshme duke i hulumtuar efektet që mund të kenë dhe arsyen pse janë duke ndodhur. Të krijohen kapacitete teknike me pajisjet dhe veglat e nevojshme që mundësojnë monitorimin proaktiv të sistemeve të TIK-ut për të përmirësuar sigurinë e tyre.

1.2 Ngritja e kapaciteteve për auditim të sistemeve të TIK-ut

Për të vlerësuar integritetin, konfidencialitetin dhe disponueshmërinë e informacionit duhet të ngritën kapacitetet për auditimin e sistemeve të TIK-ut. Po ashtu auditimi i sistemeve të TIK-ut duhet të bëhet edhe në rastin kur kërkohet të bëhet vlerësim lidhur me implementimin e politikave të sigurisë në sistemet e TIK-ut si dhe për vlerësimin e incidenteve të sigurisë kibernetike.
Kapacitetet e auditimit të sistemeve të TIK-ut në MM/FSK do të ngritën në kuadër të MM-së dhe për realizimin e detyrave dhe aktiviteteve do të bashkëpunojë ngushtë me Njësinë për mbrojtje kibernetike në SHPFSK.

1.3 Ngritja e kapaciteteve për reagim në incidente kompjuterike

Me qëllim të reagimit më të shpejtë dhe efikas në incidente kompjuterike, duhet të funksionalizohet ekipi reagues në incidente kompjuterike (CERT) në NJMK në SHP i cili do të jetë ekipi i parë reagues, me që rast do të ndjek procedurat e njoftimit dhe alarmimit të lidershipit varësisht nga përshkallëzimi i incidentit kompjuterik. Ky ekip në mënyrë aktive me kapacitetet bazë do të monitorojë vazhdimisht rrjetin për incidentet kompjuterike dhe koordinoj aktivitetet e ndërmarra për mënjanim të incidenteve me strukturat përgjegjëse të TIK-ut dhe lidershipin e MM/FSK. Në rast të incidenteve të rëndësisë së madhe dhe shkallës së lartë të përfshirjes ky ekip duhet të zgjerohet me pjesëtarë shtesë nga strukturat e sigurisë kibernetike dhe TIK-ut në MM dhe FSK. Angazhimi i këtyre pjesëtarëve në CERT do të jetë deri në zgjidhjen dhe rikuperimin e të dhënave dhe rrjetit nga incidenti. Koordinimi i aktiviteteve të CERT në nivel kombëtar dhe ndërkombëtar bëhet në bashkëpunim me strukturën përgjegjëse për mbrojtje kibernetike në MM dhe DBNIEA.
Funksionimi i plotë të punës së ekipit për reagim në incidente do të përshkruhet në Politikën dhe planin për reagim ndaj incidenteve kompjuterike.

1.4 Ngritja e kapaciteteve për vlerësimin e dobësive në sistemin e TIK-ut

Vlerësimi i dobësive në sistemin e TIK-ut të MM/FSK duhet të bëhet në vazhdimësi me qëllim të ngritjes së nivelit të sigurisë së sistemit dhe për të zvogëluar rrezikun nga kërcënimet që janë pjesë përbërëse e dobësive të identifikuara. Kjo aftësi do të ngritët në NJMK në SHP. Do të funksionalizohen veglat e nevojshme për skanim të rrjetit për të identifikuar dobësitë dhe pastaj do të kryen analiza për dobësitë e konstatuara për të vazhduar tutje me marrjen e masave për evitimin e tyre.

1.5 Mbrojta e sistemeve të TIK në MM/FSK

Për të siguruar mbrojtje të qëndrueshme ndaj rreziqeve dhe kërcënimeve të vazhdueshme kibernetike është e nevojshme të bëhet implementimi i kontrolleve kritike të sigurisë në sistemet e TIK siç janë të përshkruara nga standardet ndërkombëtare të sigurisë së sistemeve dhe informacionit. Këto kontrolle përfshijnë masa për monitorimin e vazhdueshëm të rrjeteve dhe sistemeve, zbatimin e protokolleve të autentifikimit dhe përdorimin e teknologjive të enkriptimit për të mbrojtur komunikimet dhe të dhënat sensitive.

2. NGRITJA E VETËDIJES DHE FORCIMI I NJOHURIVE NË FUSHËN E SIGURISË KIBERNETIKE BRENDA MM/FSK DUKE PËRFSHIRË REKRUTIMIN DHE MBAJTJEN E PERSONELIT TË KUALIFIKUAR

Për të arritur realizimin e objektivave në fushën e mbrojtjes kibernetike kërkohet vetëdijesimi i gjithë personelit të MM/FSK-së mbi rreziqet në fushën e sigurisë kibernetike, si dhe organizimi i trajnimeve specialistike për personelin e kësaj fushe.
Përmbushja e objektivit 2 strategjik synohet të arrihet përmes 3 objektivave specifike:

2.1 Ngritja e vetëdijesimit të pjesëtarëve të MM/FSK për rreziqet në fushën e sigurisë kibernetike

Dobësia më e madhe që çon në humbjen ose kompromet imin e informacionit është shkaktuar nga veprime të paqëllimta nga personeli, të tilla si përdorimi jo-kompetent ose i pakujdesshëm i pajisjeve të TIK-ut. Prandaj, i gjithë personeli i MM/FSK-së duhet të jetë i vetëdijshëm për rreziqet në fushën e sigurisë kibernetike. Vetëdijesimi për sigurinë kibernetike do të bëhet pjesë e integruar e kurseve trajnuese brenda FSK-së.

Trajnimi dhe vetëdijesimi për sigurinë kibernetike i gjithë personelit duhet të jetë i vazhdueshëm përmes formave të ndryshme, si:

- Trajnimi i vazhdueshëm online ose me prezencë fizike për kërcënimet dhe rreziqet në fushën e sigurisë kibernetike.
- Kampanjat e ndryshme vetëdijesuese për rreziqet e sulmeve kibernetike dhe formën e mbrojtjes nga këto sulme për gjithë personelin e MM/FSK
- Promovimi i "Muajit evropian për siguri kibernetike"
- Organizimi i seminareve për mbrojtje kibernetike për personelin e MM/FSK
- Organizimi i ushtrimeve për të vlerësuar sjelljen e personelit karshi sulmeve të ndryshme kibernetike
- Testimi i rregullt vjetor për njohuritë rreth vetëdijesimit për siguri kibernetike.

2.2 Trajnimet specialistike

MM dhe FSK duhet të zhvilloj dhe ruaj aftësitë e personelit të mbrojtjes kibernetike në parandalimin, zbulimin dhe reagimin ndaj incidenteve të mundshme kibernetike në sistemet e TIK-ut të MM/FSK. Kjo do të jetë e mundur me zhvillimin dhe organizimin e vazhdueshëm të trajnimeve dhe ushtrimeve në këtë fushë.

- Trajnimi specialistik në fushën e sigurisë dhe mbrojtjes kibernetike për personelin përgjegjës për këtë fushë
- Organizimi i ushtrimeve për të vlerësuar dhe testuar sigurinë në sistemin e TIK, si dhe testimin e personelit të kësaj fushe për reagimet ndaj incidenteve
- Organizimin dhe pjesëmarrjen në ushtrimet në fushën e sigurisë kibernetike në nivel shtetëror
- Organizimin dhe pjesëmarrjen në ushtrimet në fushën e sigurisë kibernetike me vendet e Ballkanit dhe partnerët për paqe të vendeve respektive.

2.3 Rekrutimi dhe mbajtja e personelit të kualifikuar

Zhvillimi i specialistëve në fushën e sigurisë kibernetike dhe TIK-ut në përgjithësi, kërkon kohë dhe investime. Prandaj për të eliminuar këta dy faktorë mjaft të rëndësishëm, MM/FSK gjatë kampanjave rekrutuese do të vendos kritere për pranimin e personelit të ri duke rekrutuar talentet entuziast të cilët paraprakisht kanë një përgatitje dhe njohuri solide në këtë fushë. Kjo do të ndihmonte në masë të madhe institucionin që të vazhdojë më tutje avancimin e njohurive të tyre sipas kritereve që kërkohen në përshkrimin e detyrave të punës.

Po ashtu në disa nga pozitat me personel ushtarak në fushën e mbrojtjes kibernetike që kërkohet të ketë kualifikim shumë të lartë dhe nuk kërkon angazhim të vazhdueshëm, MM/FSK duhet të mundësoj që këto pozita të rekrutoj personel rezervë dhe angazhimi i tyre të bëhet sipas nevojës. Benefitet e kësaj praktike janë të shumta si:

- Zbutja në masë të madhe e mungesës së specialistëve senior në këtë fushë;
- Zvogëlimi i barrës për buxhet shtesë për mbajtjen dhe beneficimin e kësaj kategorie të personelit;
- Këta pjesëtarë do të kenë mundësi të punojnë edhe në institucione të tjera publike dhe private, me ç'rast trajnimet dhe përvojat e marra atje do të ndikojnë pozitivisht në zhvillimin e tyre profesional për të qenë në hap për parandalimin dhe zbulimin e sulmeve kibernetike potenciale për MM/FSK.

Për të mbajtur personelin e kualifikuar në fushën e sigurisë kibernetike dhe TIK-ut në përgjithësi është e nevojshme që të bëhet një vlerësim për punën e tyre dhe të përcaktohet një shumë e të hollave financiare si beneficion për nivelin e specializimit për punën që bëjnë.

Po ashtu për çdo pjesëtarë që përfiton nga trajnimet specialistike në fushën e TIK dhe sigurisë kibernetike, pas çdo trajnimi afatgjatë të obligohet për zgjatjen e shërbimit ose kompensimin e pagesës së trajnimit sipas rregulloreve në fuqi.

3. NGRITJA DHE FUNKSIONALIZIMI I QENDRËS SHTETËRORE TRAJNUESE PËR SIGURINË KIBERNETIKE

Njëri ndër aktivitetet që ndikon në zvogëlimin e rrezikut ndaj kërcënimeve potenciale për sigurinë kibernetike është trajnimi i stafit në këtë fushë. Vetëdijesimi i gjithë personelit për rreziqet në fushën e sigurisë kibernetike si dhe trajnimi i vazhdueshëm i specialistëve të sigurisë kibernetike janë metoda më e mirë për të evituar dhe parandaluar sulmet e ndryshme kibernetike. Për këtë arsye ngritja e Qendrës Shtetërore Trajnuese për Siguri Kibernetike është njëra ndër objektivat kryesore të MM/FSK e po ashtu edhe ato të Qeverisë së Republikës së Kosovës. Kjo Qendër trajnuese do të ofrojë trajnime për të gjitha institucionet e Republikës së Kosovës, OShE dhe OShD.

Do të realizohen trajnime për vetëdijesimin e përdoruesve të pajisjeve dhe sistemeve të TI-së lidhur me rreziqet në fushën e sigurisë kibernetike, si dhe trajnime në fushën e sigurisë kibernetike përmes ushtrimeve dhe simulimeve të sulmeve me skenarë të ndryshëm. Këta skenarë ofrojnë një simulim të ushtrimeve reale që janë të mundshme për të ndodhur në sistemet e TIK-ut në RKS dhe pas realizimit do të mundësohet identifikimi dhe vlerësimi i dobësive si dhe çështjet për përmirësim.

Për formën e funksionimit të kësaj qendre do të hartohet Koncepti për ngritjen e Qendrës shtetërore trajnuese për siguri kibernetike, në të cilin dokument do të planifikohen të gjitha detajet lidhur me kapacitetet që do të ketë kjo Qendër.

Përmbushja e objektivit 3 strategjik synohet të arrihet përmes 3 objektivave specifike:

3.1 Ngritja e kapaciteteve njerëzore për trajnim

Gjatë periudhës tri vjeçare sipas prioriteteve të përcaktuara nga lidershipi i MM/FSK-së do të caktohet udhëheqësi i Qendrës, rekrutohen instruktorët dhe stafi mbështetës i planifikuar për këtë Qendër. Varësisht prej trajnimeve që kërkohen të realizohen në këtë Qendër, do të rekrutohen edhe instruktorët e trajnuar paraprakisht që janë të gatshëm për realizimin e trajnimeve. Përveç instruktorëve të përhershëm në QSHTSK do të ketë mundësi të angazhohen edhe instruktorë brenda institucioneve shtetërore, instruktorë nga sektori privat dhe instruktorë ndërkombëtar. Kushtet dhe forma e angazhimit është e përcaktuar në Rregulloren për detyrat dhe përgjegjësitë e Qendrës Shtetërore Trajnuese për Siguri kibernetike.

3.2 Hartimi i programeve trajnuese

Në bashkëpunim me ASK do të hartohen kurrikula të përbashkëta të trajnimit me qëllim të harmonizimit të trajnimeve dhe ushtrimeve për siguri kibernetike për MM/FSK, institucionet tjera qeveritare, OShE dhe OShD. Organizimi i këtyre trajnimeve do të bëhet më qëllim të ngritjes së kapaciteteve njerëzore për përmirësimin e sigurisë kibernetike në vend. Përveç trajnimeve specialistike do të realizohen edhe ushtrime në fushën e sigurisë kibernetike ndërinstitucionale duke përfshirë sektorin publik, OShE dhe OShD.

Po ashtu në koordinim me institucionet e ASK do të hartohen skenarët dhe realizohen ushtrime të përbashkëta, përmes së cilave institucionet e përfshira do të testojnë kapacitetet e tyre në reagim ndaj kërcënimeve kibernetike. Mbajtja e këtyre ushtrimeve do të përmirësoj kapacitetet në reagim ndaj kërcënimeve të ndryshme, qoftë në nivel institucional apo në nivel vendi.

3.3 Ngritja e kapaciteteve teknike për trajnim

Për simulimin dhe organizimin e ushtrimeve në fushën e sigurisë kibernetike do të ngritët Laboratori për testime dhe trajnime (Cyber Range) i cili do të mundësojë ngritjen profesionale të personelit të sigurisë kibernetike për të parandaluar, hetuar dhe mënjanuar sulmet kibernetike. Po ashtu do të funksionalizohen veglat e ndryshme për monitorim, testim dhe vlerësim të dobësive në rrjet të cilat do të ndihmojnë realizimin e testimeve dhe ushtrimeve të ndryshme.

4. IDENTIFIKIMI DHE MBROJTJA E INFRASTRUKTURËS KRITIKE TË INFORMACIONIT

Identifikimi dhe mbrojtja e infrastrukturës kritike të informacionit është e rëndësisë së veçantë për MM dhe FSK që të kryej detyrat sipas misionit, pasi që çrregullimi apo dëmtimi i kësaj infrastrukture mund të ketë pasoja të mëdha në funksionimin dhe përmbushjen e misionit sipas obligimeve kushtetuese.

Përmbushja e objektivit 4 strategjik synohet të arrihet përmes 2 objektivave specifike:

4.1 Identifikimi i infrastrukturës kritike të informacionit

Identifikimi i infrastrukturës kritike të MM/FSK është një proces mjaft i rëndësishëm për institucionin dhe vendin në përgjithësi. Sipas Ligjit Nr. 06/L-014 për infrastrukturë kritike kërkohet bashkëpunim i të gjitha institucioneve të RKS që posedojnë infrastrukturë kritike për të identifikuar dhe më pas të marrin të gjitha masat për të mbrojtur atë. Po ashtu duhet të ndjeken kriteret e parapara në këtë Ligj për identifikimin dhe mbrojtjen e infrastrukturës që janë në harmoni edhe me dokumentin e ENISA-së për identifikimin e IKI.
Për identifikimin e infrastrukturës kritike të informacionit duhet të përcaktohen shërbimet e domosdoshme ose kritike për kryerjen e detyrave sipas misionit, pastaj të identifikohet infrastruktura e domosdoshme që mbështet funksionimin e atyre shërbimeve.
MM/FSK do të ndjek udhëzimet nga Grupi Punues për Sigurinë Kibernetike në Infrastrukturës Kritike për identifikimin dhe përcaktimin e infrastrukturës kritike brenda institucionit.
Trendi i zhvillimit dhe avancimit me ritëm të shpejtë i teknologjisë informative bënë që infrastruktura kritike e informacionit në MM/FSK të pësoj ndryshime të kohëpaskohshme. Për këtë arsye është shumë e vështirë të përcaktohet se cila pjesë e infrastrukturës është më pak kritike dhe cila më shumë. Prandaj identifikimi i infrastrukturës kritike duhet të jetë proces i vazhdueshëm.

4.2 Mbrojtja e infrastrukturës kritike

Pas identifikimit dhe hartimit të listës me infrastrukturën kritike në MM/FSK, duhet të merren të gjitha masat dhe veprimet e nevojshme për mbrojtjen e kësaj infrastrukture. Pra duhet të bëhet:

- Përcaktimi i kritereve dhe niveli i mbrojtjes për secilin kategori të infrastrukturës kritike;
- Përmirësimin e sistemeve të monitorimit dhe identifikimit të ndërhyrjeve në infrastrukturën kritike në nivel të FSK-së;
- Kontrollimi i vazhdueshëm i këtyre kritereve dhe nivelit të mbrojtjes krahas zhvillimit të teknologjisë dhe ndryshimit të mjedisit të sigurisë.

Forcimi i mbrojtjes kibernetike të MM dhe FSK konsiston në mbrojtjen e sistemeve të cilët janë të kërcënuar ndaj sulmeve dhe ndërprerjeve në dy drejtime, si nga jashtë ashtu edhe nga brenda, nëpërmjet monitorimit, analizës së trafikut të të dhënave, detektimit të sulmeve kibernetike dhe përgjigjen ndaj tyre.
Pavarësisht ngritjes së nivelit të mbrojtjes së sistemeve të TIK-ut, gjithnjë duhet të kemi parasysh dhe me një fokus të veçantë të vëzhgimit të ndërmarrjes së masave të sigurisë kibernetike të infrastrukturës kritike që ndërlidhet me operacionet ushtarake që janë në pronësi qoftë nga institucionet publike ose private.

5. INTENSIFIKIMI I BASHKËPUNIMIT KOMBËTAR DHE NDËRKOMBËTAR

Përmes kësaj strategjie MM/FSK në vazhdimësi do të tentoj të rris bashkëpunimin me institucionet vendore dhe ndërkombëtare për t'iu përgjigjur sfidave dhe mundësive të reja në fushën e mbrojtjes kibernetike. Kryerja e detyrave sipas misionit në fushën e mbrojtjes kibernetike kërkon bashkëpunim të ngushtë me partnerët bilateral të MM/FSK. Një nga angazhimet e MM/FSK është avancimi i bashkëpunimit për shkëmbim të përvojave dhe informacionit për reagim në incidente kompjuterike në fushën e sigurisë dhe mbrojtjes kibernetike me institucionet tjera të sigurisë të RKS-së. Shkëmbimi i informacionit dhe eksperiencave me institucionet vendore dhe ndërkombëtare synohet të jetë i vazhdueshëm me qëllim të ndërtimit të besimit dhe bashkëpunimit ndërinstitucional për përmirësimin e sigurisë së hapësirës së përbashkët kibernetike. Ngritja e bashkëpunimit synohet të bëhet përmes pjesëmarrjes dhe organizimit të aktiviteteve të ndryshme për siguri kibernetike: si seminare, konferenca dhe ushtrime të përbashkëta për reagim në incidente kibernetike.

Përmbushja e objektivit 5 strategjik synohet të arrihet përmes 2 objektivave specifike:

5.1 Bashkëpunimi me institucionet vendore

Me avancimin e teknologjisë informative, rreziku i sigurisë kibernetike shfaqet në forma të ndryshme si pasojë e aktiviteteve të grupeve kriminale, terroriste, hakerëve në nivel global, e që këto veprime dashakeqe mund të ndodhin edhe në Kosovë. Prandaj siguria kibernetike kërkon vëmendje më të lartë dhe aktive nga nivelet e larta të institucioneve shtetërore. Kjo e bënë që siguria kibernetike të varet nga mundësitë dhe aftësitë e vetë shteteve dhe institucioneve të tyre për të mbrojtur hapësirën kibernetike. Siguria kibernetike është një fushë në të cilën të gjitha institucionet publiko-private apo civile e ushtarake brenda dhe jashtë vendi, duhet të veprojnë në të njëjtën kohë dhe të kenë një bashkëpunim reciprok. Pa dallim vendi, teknikat e përdorura nga sulmuesit e hapësirës kibernetike kryesisht janë të ngjashme për të shfrytëzuar dobësitë e përgjithshme të sistemeve të TIK-ut. Arritja dhe hartimi i marrëveshjeve të bashkëpunimit me institucionet tjera shtetërore dhe private për shkëmbimin e informacionit dhe eksperiencave do të ndikojë në përmirësimin dhe garantimin e sigurisë dhe rritjen e besueshmërisë për hapësirën kibernetike në nivel vendi. Po ashtu arritja e një bashkëpunimi të ngushtë me sektorin privat në fushën e kërkimit, zhvillimit dhe trajnimit të personelit është e domosdoshme. Duke pasur parasysh mungesën e personelit të kualifikuar në fushën e sigurisë kibernetike dhe me mundësitë e limituara buxhetore, realizimi i këtij bashkëpunimi do të jetë efikas në kuadrin e intensifikimit të bashkëpunimit në nivel vendi.

5.2 Bashkëpunimi ndërkombëtar

Një nga objektivat e MM-së ka qenë ngritja dhe ruajtja e bashkëpunimit me vendet mike me qëllim të ngritjes së kapaciteteve në fushën e sigurisë kibernetike përmes shkëmbimit të përvojave dhe njohurive. Vendi ynë respektivisht MM-ja ka arrite marrëveshje partneriteti me Gardën Kombëtare të Shtetit të IOWA që nga Marsi 2011, ku përmes këtij programi do të ndërtohet bashkëpunimi në aspektin e sigurisë e kryesisht në fushat kritike. Si rezultat i këtij bashkëpunimi MM-ja dhe FSK-ja ka bërë hartimin dhe implementimin e rekomandimeve të dhëna nga ekipi për mbrojtje kibernetike i Gardës Kombëtare të Shtetit të IOWA-së lidhur me funksionalizimin e sigurisë kibernetike në FSK. Synimi është që të arrihet bashkëpunim edhe me shtetet tjera bilaterale për

shkëmbim të informacionit dhe ndërveprueshmëri në zgjidhjen më efikase të incidenteve kompjuterike në rastet kur në incident janë të përfshirë edhe shtetet tjera.

Po ashtu kjo Strategji synon listimin, akreditimin dhe anëtarësimin e ekipeve të specializuara në fushën e sigurisë kibernetike në organizatat ndërkombëtare në këtë fushë dhe reagimit në incidente kompjuterike në veçanti.

IX. MONITORIMI DHE RAPORTIMI MBI ZBATIMIN E PLANIT TË VEPRIMIT

Procesi i zbatimit të strategjisë për mbrojtje kibernetike ka për synim realizimin e objektivave strategjike, objektivave specifike dhe aktiviteteve tjera në kuadër të sigurisë kibernetike. Pasi që siguria e informacionit është detyrë kryesore e strukturave të MM-së dhe FSK-së, atëherë përcjellja, zbatimi dhe monitorimi në vazhdimësi i kësaj strategjie kërkon koordinim dhe bashkëpunim të ngushtë dhe efektiv në mes strukturave përgjegjëse për siguri kibernetike të MM/FSK me agjencitë dhe institucionet tjera të vendit dhe ato ndërkombëtare.

Siguria e informacionit dhe sistemeve të TIK-ut duhet të jetë aktivitet i përditshëm i mbështetur, monitoruar dhe kontrolluar nga çdo strukturë e nevojshme e MM/FSK për sigurinë e informacionit.

Departamenti i Komunikimit dhe Teknologjisë Informative (G6) në SHPFSK është përgjegjës për hartimin e Planit të veprimit për zbatimin e Strategjisë për Mbrojtje Kibernetike.

Departamenti i Komunikimit dhe TI-së është përgjegjësi kryesor në përcjelljen dhe monitorimit për zbatimin e Planit të veprimit të Strategjisë për Mbrojtjen Kibernetike në MM/FSK.

Departamentet, sektorët dhe njësitë e FSK-së të përfshira në Planin e Veprimit të kësaj Strategjie do të dorëzojnë në Departamentin e Komunikimit dhe TI-së në MM raportet e tyre periodike tremujore për realizimin e aktiviteteve të paraqitura në këtë plan. Departamenti për Komunikim dhe TI në MM do të hartojë raportin e përmbledhur për të gjitha aktivitetet e planifikuara për fazën e raportimit për Ministrin e Mbrojtjes, Komandantin e FSK-së dhe Sekretarin e Përgjithshëm në MM.

Me qëllim të zbatimit sa më mirë të Strategjisë për mbrojtje kibernetike duhet që për çdo vit të bëhet analiza dhe vlerësimi i zbatimit të Strategjisë për mbrojtje kibernetike. Bazuar në analizën dhe vlerësimin e realizimit të aktiviteteve të bëhet rishikimi dhe plotësimi i planit të veprimit të kësaj Strategjie.

X. PËRFUNDIMI

Mbrojtja kibernetike kërkon një qasje gjithëpërfshirëse të të gjithë akterëve të MM/FSK për arritjen e objektivave e Strategjisë për mbrojtje kibernetike.

Rritja e ndërgjegjësimit ndaj përgjegjësive të përbashkëta dhe marrja e masave të duhura në fushën e sigurisë së informacionit do të garantoj hapësirë më të sigurt kibernetike në MM/FSK.

Implementimi dhe zbatimi i objektivave të paraparë në këtë strategji do të siguroj që MM dhe FSK të jenë në gjendje për të vepruar në mënyrë efektive dhe efikase në fushën e sigurisë kibernetike.

E rëndësishme është edhe krijimi i partneriteteve me institucionet qeveritare dhe ato të sektorit privat që janë pronar të infrastrukturës kritike, për të ndarë përvoja dhe informacione që konsiderohen të rëndësishme për të parandaluar dhe mënjanuar kërcënimet kibernetike. Po ashtu, është i rëndësishëm edhe bashkëpunimi me vendet e rajonit dhe vendet e tjera partnere, me qëllim marrjen e masave parandaluese për të minimizuar rreziqet kibernetike dhe për krijimin e një fronti të bashkuar që do të bëjë të ulen këto rreziqe.

Ngritja e QSHTSK si njëra nga objektivat strategjike të kësaj strategjie do të ndikojë në rritjen e numrit të ekspertëve në fushën e mbrojtjes kibernetike, nëpërmjet organizimit të shpeshtë të ushtrimeve dhe trajnimeve të specializuara.

Në përfundim të kësaj logjike, është detyrimi ynë për të njohur, përgatitur dhe trajnuar çdo nivel të MM/FSK, për t'iu kundërvënë kërcënimeve kibernetike, si një kërkesë dhe domosdoshmëri strategjike në një epokë të konflikteve digjitale.