R E P U B L I K A E S H Q I P Ë R I S Ë
MINISTRIA E MBROJTJES

STRATEGJIA PËR MBROJTJEN KIBERNETIKE

(CYBER DEFENSE)

HYRJE

Në Strategjinë e Sigurisë Kombëtare përcaktohet se: "Shqipëria renditet ndër vendet ku zhvillimi i telekomunikacionit, qasja në internet dhe informatizimi i shoqërisë përparon shumë shpejt. Rritja e komunikimit përbën një vlerë të shtuar në zhvillimin ekonomik dhe shoqëror të vendit, por në të njëjtën kohë, ajo e ekspozon atë ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe jo shtetërorë. Sulmet kibernetike kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike".[1]

Asetet dixhitale në rritje janë pjesë integrale e operacioneve ushtarake, ndërkohë, rritja e varësisë së punës nga asetet dixhitale, krijon kërcënime të mjedisit të sigurisë kibernetike. Me Siguri Kibernetike do të kuptojmë: kushtet në të cilat hapësira kibernetike[2] është e mbrojtur në lidhje me ngjarjet aksidentale ose me vetëdashje të cilat konsistojnë në marrjen dhe transferimin e të dhënave, në modifikimin e tyre, shkatërrimin ose bllokimin e paligjshëm të sistemeve të komunikimit e të informacionit, për shkak të masave të papërshtatshme të sigurisë.

Fusha dixhitale e hapësirës kibernetike është fusha e pestë e operacioneve ushtarake në botë, së bashku me ajrin, detin, tokën dhe hapësirën.

Teknologjia e komunikimit dhe e informacionit i mundëson Ministrisë së Mbrojtjes dhe Forcave të Armatosura (MM/FA) efikasitetin në Komandim - Kontroll (C2), mbështetje logjistike dhe shërbime të tjera të cilat janë të mbështetura në sistemet e komunikimit dhe informacionit.

Kjo strategji e promovuar nga MM synon: mbajtjen e një mjedisi operimi elektronik të sigurtë, të qëndrueshëm dhe të besueshëm, i cili mbështet sigurinë në strukturat e MM/FA dhe rrit përfitimet e mjedisit dixhital për to; vendosjen e standardeve për përdorimin e sigurtë të hapësirës kibernetike; inkurajimin për një zbatim gjithëpërfshirës; garantimin e sigurisë dhe progresit për strukturat dhe sistemet e ndërlidhjes dhe informacionit (SNI) të MM.

Strategjia e Sigurisë Kibernetike përshkruan sfidat aktuale në çështje të sigurisë të sistemeve të ndërlidhjes dhe informacionit (SNI) dhe pikat kryesore me qëllim për të përballuar këto sfida.

Një sërë faktorësh si shpejtësia e zhvillimeve teknologjike, dinamika dhe kompleksiteti i shfrytëzimit të hapësirës kibernetike, e vendosin Ministrinë e Mbrojtjes dhe FA përpara sfidave reale për ngritjen e kapaciteteve për mbrojtjen kibernetike, të shoqëruar me politika, udhëzime, procedura koordinuese e monitoruese. Për rrjedhojë, Strategjia e Mbrojtjes Kibernetike do të rishikohet në përshtatje me këto ndryshime.

---

[1] "Strategjia e Sigurisë Kombëtare", Tiranë , Korrik 2014 , faqe 23

[2] ***Hapësirë kibernetike*** *– konsiderohet hapësira virtuale globale e të gjithë sistemeve të Informacionit të ndërlidhur në nivel global të dhënash .(sipas draftit të strategjisë Kombëtare)*

I. TË PËRGJITHSHME

Përparësia kryesore e Strategjisë së Mbrojtjes kibernetike do të jetë trajtimi i hapësirës kibernetike si një fushë (domain) operacionale me qëllim për t'u organizuar, trajnuar dhe pajisur me mjete, në mënyrë që MM/FA të mund të veprojë në potencialin e hapësirës kibernetike për mbrojtjen e sistemeve të ndërlidhjes dhe të informacionit.

Qëllimi kryesor i saj është të sigurojë orientime, koherencë dhe fokus, për një qasje gjithëpërfshirëse, për të zhvilluar kapacitetet ushtarake në hapësirën kibernetike në tre vitet e ardhshme.

Ministria e Mbrojtjes përcakton sigurinë kibernetike nëpërmjet masave në lidhje me konfidencialitetin, disponibilitetin dhe integritetin e informacionit që trajtohet, përpunohet, ruhet, transmetohet dhe komunikohet me mjetet elektronike.

Vendosja dhe zbatimi i këtij prioriteti për MM/FA, përcakton nevojën në:

- Menaxhimin e riskut të hapësirës kibernetike përmes përpjekjeve të vazhdueshme për rritjen e nivelit të trajnimit, sigurimin e informacionit, informimit më të konsoliduar për situatën dhe duke krijuar mjedis të sigurt dhe sisteme të qëndrueshme.
- Garantimin e integritetit dhe disponibilitetit të sistemeve nëpërmjet bashkëpunimit dhe mbrojtjes kolektive duke mbajtur pamje operacionale të përbashkët.
- Garantimin e kapaciteteve të integruara, duke bashkëpunuar ngushtë me Komandat e FA, Shërbimet dhe Agjencitë për vendosjen e kapaciteteve të reja atje ku ato nevojiten më shumë.

Strukturat përkatëse të sistemeve të ndërlidhjes dhe informacionit (SNI) të MM/FA punojnë në mënyrë aktive për të siguruar infrastrukturë të sigurt për këto sisteme, nëpërmjet organizimit, alokimit të burimeve të duhura, kushteve të përgjithshme të mira dhe masa efektive. Këto struktura integrojnë sigurinë dhe forcat në infrastrukturën e informacionit për të mbrojtur veprimtarinë e MM dhe FA si dhe të gjithë përdoruesit e këtyre sistemeve.

Strategjia e Mbrojtjes Kibernetike do të ketë përputhshmëri me kërkesat që shtrohen vazhdimisht në këtë fushë dhe do të respektojë të gjitha parimet e parashikuara në konventat, marrëveshjet ndërkombëtare, iniciativat që do të ndërmerren, me synimin që të mbrojë dhe parandalojë ndërhyrjen ose dëmet në Sistemet e Ndërlidhjes dhe Informacionit (SNI).

Kjo Strategji do të fokusohet në :

- Masa për të adresuar kërcënimet që drejtohen ndaj sistemeve të ndërlidhjes dhe informacionit (SNI) të MM dhe FA.
- Masa ndërgjegjësuese për krimin kibernetik.
- Masa për të ndërtuar besimin dhe sigurinë në përdorimin e sistemeve të ndërlidhjes dhe informacionit (SNI) të MM dhe FA.
- Zhvillimi, rishikimi dhe rifreskimi i politikave, rregullave, udhëzimeve dhe procedurave ekzistuese për të siguruar përputhshmëri me kërkesat aktuale.

II. SFIDAT E SIGURISË

Sfidat e sigurisë për Sistemet e Ndërlidhjes dhe Informacionit (SNI) përfshijnë të gjitha nivelet e strukturave të MM dhe FA duke filluar nga pajisjet individuale, që përdoren në mjediset zyrtare 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 përfshijnë:

Interneti dhe pajisjet mobile: Përdorimi gjithnjë e në rritje i internetit dhe i sistemeve të reja kompjuterike, sistemet industriale të kontrollit, telefonat mobile, pajisjet magazinuese të lëvizshme (memory stick), mediat sociale dhe tabletat, na bëjnë më shumë efiçent por edhe më shumë të pambrojtur në mjedisin ku ushtrojmë detyrat funksionale.

Shkëputja - ndërprerja e sistemeve gjithnjë në rritje është një çështje kritike: Strukturat e MM dhe të FA, si e gjithë shoqëria, janë bërë shumë të pambrojtur kundrejt shkëputjeve, ndërprerjeve të shkurtra të sistemeve ose rrjeteve, duke rritur kështu rëndësinë e të pasurit një infrastrukturë të sigurt dhe të fuqizuar për sistemet e ndërlidhjes dhe informacionit (SNI).

Platformat me shërbime të reja dhe mungesa e qartësisë për to: Përdorimi gjithnjë e në rritje i platformave të reja të shërbimeve, siç janë mënyrat dhe mjetet kompjuterike online ose "cloud", me zgjidhje jo të qarta dhe transparente, e bëjnë shumë më të vështirë vlerësimin e rrezikut nga ana e përdoruesve, në sistemet që ata përdorin.

Përdorimi gjithnjë e në rritje i komunikimit dhe transmetimit të informacionit jashtë mjedisit të punës: MM dhe FA nuk janë rrjete të mbyllura në një mjedis të kufizuar. Puna dhe funksionet e strukturave janë të lidhura me struktura të tjera të administratës publike por edhe përtej kufijve të vendit edhe në kontinente të tjera. Kjo përbën një sfidë më vete për shkak të kushteve, rrezikut të dyanshëm, ligjeve e rregullave të ndryshme, mungesës së transparencës në lidhje me këto rregulla, të cilat e bëjnë shumë të vështirë që strukturat e MM dhe FA të ushtrojnë kontroll mbi to.

Krijimi i marketit të krimit kibernetik: Interneti dhe pajisjet mobile kanë krijuar dhe drejtuar në një rrezik më të madh, duke qenë të zbuluar ndaj krimit kibernetik. Sot është zhvilluar një market i nëndheshëm, i padukshëm, i aksesueshëm lehtësisht në internet, për blerje dhe shitje informacioni si dhe tregëtimin e mjeteve për krimin kibernetik. Kriminelët po e shfrytëzojnë këtë mundësi gjithnjë e më shumë.

Një kërcënim në rritje është spiunazhi dhe sabotazhi, një drejtimi i ndërhyrjeve (hacking) profesionale ndaj sistemeve të ndërlidhjes dhe informacionit. Objektivat ushtarakë janë e do të jenë gjithnjë e më shumë pikësynim i sulmeve, për këtë arësye shumë vende kanë ose janë duke zhvilluar kapacitete për spiunazh dhe luftë elektronike ndaj sistemeve të informacionit dhe të komunikimit.

Punonjës jo korrekt dhe të besueshëm. Shkeljet e brendshme, vjedhja ose keqpërdorimi i burimeve të sistemeve të komunikimit dhe informacionit nga vetë punonjësit e institucionit janë vështirë të zbulohen. Kjo vjen për shumë arsye, duke përfshirë procedura të dobëta operimi dhe menaxhimi të sistemeve, një mos përcaktim të qartë dhe të saktë të përgjegjësive në këtë fushë, privilegjet që duhet të kenë punonjësit në sisteme etj. Sulmi i brendshëm në sisteme e bën edhe më të vështirë zbulimin e sulmeve të jashtme.

Abuzimi me privatësinë dhe identitetin: Privatësia personale është gjithashtu e kërcënuar 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 autoritetet institucional.

III. OBJEKTIVAT KRYESORË DHE PRIORITETET STRATEGJIKE

Mbështetur në sfidat e sigurisë ndaj sistemeve të ndërlidhjes dhe të informacionit, Ministria e Mbrojtjes ka identifikuar katër objektiva kryesorë për sigurinë e informacionit dhe të sistemeve të komunikimit, në të cilat ky informacion trajtohet, përpunohet, ruhet apo transmetohet:

- Koordinim më të mirë dhe kuptim të përbashkët të situatës kibernetike.
- Kryerja e vlerësimit dhe analizës së riskut brenda vitit 2015, për të përcaktuar masat e nevojshme për mbrojtjen minimale.
- Krijimi i aftësive dhe kapaciteteve më të mira për të trajtuar situata të ndryshme në sistemet e komunikimit e të informacionit.
- Zbatimi i detyrimeve për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit.

Këto objektiva të përgjithshme për sigurinë e sistemeve të komunikimit dhe të informacionit do të trajtohen njëkohësisht, të ndërvarur nga njëri-tjetri si faktorë suksesi.

Objektivat e mësipërm do të realizohen përmes gjashtë shtyllave strategjike, si më poshtë:

1. ***Adoptimi i një qasjeje gjithëpërfshirëse dhe sistematike në sigurinë e Sistemeve të Ndërlidhjes dhe Informacionit***.

2. ***Forcimi i mbrojtjes kibernetike të M/M dhe FA nëpërmjet përmirësimit të infrastrukturës së Sistemeve të komunikimit dhe të informacionit.***

3. ***Forcimi i pozitës së njohurive dhe inovacionit të Ministrisë së Mbrojtjes për Hapësirën Kibernetike nëpërmjet ndryshimit të kulturës, ndërgjegjësimit dhe edukimit të të gjithë punonjësve në strukturat e MM/FA, mjeteve praktike për të mbrojtur sistemet e komunikimit dhe të informacionit që ata përdorin për të kryer detyrat funksionale.***

4. ***Ruajtja dhe zhvillimi i aftësive të përdoruesve dhe specialistëve për të zbuluar, trajtuar, lajmëruar dhe reaguar ndaj incidenteve që ndodhin në Sistemet e Ndërlidhjes dhe Informacionit.***

5. ***Forcimi i pozicionit të inteligjencës në Hapësirën Kibernetike.***

6. ***Intensifikimi i bashkëpunimit në nivel kombëtar dhe ndërkombëtar, partneritetit me biznesin e TI për të garantuar siguri dhe qëndrueshmëri në infrastrukturë, në rrjetet kompjuterike, në produktet që merren dhe në shërbimet që ofrohen.***

1. Adoptimi i një qasje gjithëpërfshirëse.

Objektivi i kësaj shtylle deri në vitin 2017, do të jetë mbështetja dhe riformimi i kapaciteteve operacionale kibernetike, nëpërmjet fuqizimit të aseteve kibernetike, në të gjithë veprimtaritë e FARSH si: komandim-kontrolli; logjistikë; inteligjencë; menaxhim i burimeve të mbrojtjes dhe të fushave të ndryshme funksionale. Në qendër të këtij objektivi do të jenë: Sistemet e ndërlidhjes dhe informacionit (SNI), arkitektura e tyre komplekse teknologjike, ndërveprimi midis elementeve dhe fushave funksionale të automatizuara dhe integrimi midis tyre.

Operacionet ushtarake do të përfshijnë gjithnjë e më shumë përdorimin e aftësive operative kibernetike, kryesisht në mbështetje të operacioneve të rregullta të forcave të armatosura, por edhe si një kapacitet i veçantë. Aftësitë kibernetike operative duhet të bëhen pjesë integrale e aftësisë së përgjithshme ushtarake të FARSH dhe për realizimin e këtij objektivi, investimi i MM do të përqendrohet tek përforcimi i aftësive të saj kibernetike nëpërmjet burimeve njerëzore, materiale dhe financiare.

Strukturat e MM dhe FA, si dhe personeli, duhet të përfshihen në mbrojtjen e sigurisë të sistemeve të komunikimit dhe të informacionit në mënyrë sistematike. Kjo do të sjellë një përdorim dhe menaxhimi të ndërgjegjshëm të këtyre sistemeve, si pjesë e drejtimit të përgjithshëm të institucionit nëpërmjet aplikimit dhe zbatimit të standardeve të njohura.

Në situatën aktuale është e domosdoshme dhe kritike të kryhet vlerësimi i riskut për sistemet e MM dhe të FA mbi baza reale. Për të realizuar këtë vlerësim kërkohet një angazhim serioz dhe gjithëpërfshirës i strukturave drejtuese të fushës në MM dhe SHPFA. Aktualisht, vlerësimi i riskut është jo i plotë. Nga verifikimet mbi zbatueshmërinë e masave të sigurisë në sistemet e informacionit ato janë josistematike, janë fragmentare, jo të shtrira në të gjithë mjedisin e sistemeve dhe nuk kanë mbështetje në drejtimin e administrimit. Zbatimi dhe përdorimi i standardeve aktuale dhe ato ndërkombëtare do të kontribuojë më shumë, për të vendosur sigurinë e sistemeve të ndërlidhjes dhe informacionit mbi baza gjithëpërfshirëse dhe sistematike.

Strukturat e MM dhe FA, që administrojnë sistemet e komunikimit dhe të informacionit, duhet të kenë një sistem të menaxhimit të sigurisë. Ky menaxhim duhet të ndërtohet dhe të zbatohet mbështetur në standarde të njohura të sigurisë së sistemeve dhe në përputhje me iniciativat dhe angazhimet ndërkombëtare të vendit tonë. Menaxhimi i sistemeve të ndërlidhjes dhe informacionit do të organizohet mbështetur në rreziqet që përballen aktualisht sistemet e MM dhe FA.

Gjithashtu në fokus do të jetë vendosja e kapaciteteve në dispozicion të komandimit operacional brenda vitit 2017, për të përthithur aftësitë e inteligjencës, për të mbledhur dhe proceduar informacionin kibernetik, në mënyrë që të realizohet procesi i vendim-marrjes në kohë reale. Ky objektiv do të mundësojë përballimin e dy kërcënimeve, si kundër rrjeteve dhe sistemeve miqësore, si edhe shfrytëzimin e dobësive të kundërshtarit.

Ndërgjegjësimi i mirë i situatës për hapësirën kibernetike është pjesë e ndërgjegjësimit të situatës së përgjithshme të linjës së komandimit.

2. Forcimi i mbrojtjes kibernetike të M/M dhe FA nëpërmjet përmirësimit të infrastrukturës së Sistemeve të komunikimit dhe të informacionit.

Në përgjithësi, Sistemet e Ndërlidhjes dhe Informacionit të MM/FA janë konceptuar dhe ndërtuar në përputhje me kriteret themelore: *teknologji moderne* për menaxhimin e informacionit, *funksionim dhe shfrytëzim i integruar* dhe *ndërveprueshmëri* me Sistemet e NATO-s dhe të vendeve të tjera anëtare të saj. Funksionimi i sistemeve të FA është i lidhur ngushtë me aplikimin dhe zbatimin e masave të sigurisë së informacionit. Këtij qëllimi i kanë shërbyer konceptimi i arkitekturës dhe ndërtimi i sistemeve sipas dy nënkategorive kryesore; krijimi i infrastrukturës së komunikimit/transmetimit me mjedise transmetimi pronë e MM/FA dhe monitorimi i funksionimit të rrjeteve, akreditimi, hartimi i politikave dhe procedurave të operimit në sistem.

Forcimi i mbrojtjes kibernetike të MM dhe FA konsiston në "**Mbrojtjen e rrjeteve dhe sistemeve të cilët janë të kërcënuar ndaj sulmeve dhe ndërprerjeve në dy drejtime, si nga jashtë dhe nga brenda, nëpërmjet monitorimit, analizës së trafikut të të dhënave, detektimit të sulmeve kibernetike dhe përgjigjen ndaj tyre**".

Pavarësisht arritjeve në fushën e mbrojtjes së sistemeve dhe të rrjeteve, duhet të përqendrohemi te menaxhimi i infrastrukturës së komunikimit dhe informacionit në tërësi, në lidhjet midis rrjeteve, kontrollit të hyrjeve të autorizuara ose të paautorizuara dhe mbajtjen në kontroll të vijueshëm të kapaciteteve të transmetimit të MM/FA, të cilat sigurohen nga kompanitë publike dhe private të telekomunikacionit.

Zhvillimi teknologjik bën të mundur që infrastruktura e sistemeve të informacionit dhe të komunikimit të jetë vazhdimisht në ndryshim. Për këtë arësye, është shumë e vështirë të përcaktosh pjesë të infrastrukturës së sistemeve të informacionit si pjesë kritike dhe të tjera më pak kritike, rrjedhimisht ato ndikojnë në sigurinë e përgjithshme të MM dhe FA dhe në atë kombëtare.

Prandaj, në mbështetje të këtij prioriteti duhet:

- Kryerja e vlerësimit dhe analiza e riskut, për të përcaktuar masat e nevojshme për mbrojtjen minimale brenda vitit 2015.
- Zbatimi dhe verifikimi i një pakete të plotë të masave të sigurisë, duke përfshirë personelin, sigurinë fizike dhe të sistemeve të informacionit.
- Vendosja e një regjimi të konsoliduar dhe rigoroz brenda vitit 2015 për informacionin e klasifikuar dhe hartimin e një pakete të masave të sigurisë për atë të paklasifikuar, brenda vitit 2014.
- Ngritja e kapaciteteve njerëzore, duke përmirësuar njohuritë dhe depërtimin në dobësitë dixhitale dhe duke forcuar mbikëqyrjen e zhvillimit, zinxhirin e furnizimit dhe përdorimin e komponentëve të IT-së.
- Ndërtimi i sistemit të menaxhimit të sistemeve të ndërlidhjes dhe informacionit, duke u përqendruar si tek mbrojtja e infrastrukturës kibernetike (pasiv) dhe tek përgjigjja ndaj çdo sulmi (aktiv) duke përdorur burimet njerëzore, logjistike apo financiare që kemi në dispozicion.
- Ndërgjegjësimi për Sigurinë kibernetike, duhet të bëhet një pjesë e integruar e të gjitha trajnimeve të personelit të Ministrisë së Mbrojtjes.

- Investimet në infrastrukturë dhe pajisjet e sistemeve të ndërlidhjes dhe informacionit, do të shoqërohen me investimet e duhura në fushën e sigurisë së sistemeve dhe rrjeteve (për software dhe hardware të veçantë dhe për mbrojtjen kriptografike).

- Prokurimi apo zhvillimi i sistemeve të reja, të bëhet duke marrë në konsideratë rreziqet e mundshme të përcaktuara më parë, të cilat lidhen me besueshmërinë e këtyre sistemeve dhe kërkesat operacionale që mbështesin sigurinë dhe masat konkrete të sigurisë.

3. *Forcimi i pozitës së njohurive dhe inovacionit të Ministrisë së Mbrojtjes për Hapësirën Kibernetike nëpërmjet ndryshimit të kulturës, ndërgjegjësimit dhe edukimit të të gjithë punonjësve në strukturat e MM/FA, mjeteve praktike për të mbrojtur sistemet e komunikimit dhe të informacionit që ata përdorin për të kryer detyrat funksionale.*

Kërcënimi më i rrezikshëm që çon tek humbja (potenciale) ose kompromentimi i informacionit, shkaktohet nga veprimet e paqëllimshme nga ana e personelit ashtu si edhe nga pakujdesia e përdorimit të aseteve të IT. Personeli i mbrojtjes duhet të jetë i vetëdijshëm për rrezikun që shoqëron përdorimi i aseteve dixhitale. Në kuadër të kësaj duhet theksuar:

- Zotërim i njohurive të nevojshme për të ndjekur zhvillimet përkatëse dhe për t'iu përgjigjur sulmeve në mënyrë të shpejtë dhe efektive. Ky objektiv realizohet nëpërmjet investimit në njerëz, teknologji, kërkim dhe zhvillim, me qëllim që të jetë i aftë të prokurojë, zhvillojë dhe zbatojë kapacitetet e nevojshme kibernetike në kohë reale.
- Garantimin e funksionimit normal të sistemeve, rrjeteve të komunikimit dhe të informacionit brenda vitit 2017, nëpërmjet rishikimit, modifikimit, zhvillimit dhe zbatimit të një sistemi masash sigurie. Ky orientim duhet të përqendrohet në: përcaktimin e masave shtesë të sigurisë në mënyrë që të garantohet vijimësia e funksionimit të sistemeve të komunikimit dhe të informacionit (përveç atyre të përcaktuara në kërkesat e sigurisë dhe mbrojtjes së sistemeve); përcaktimin e funksionalitetit minimal të kërkuar për infrastrukturën dhe sigurimin e funksionimit në një situatë krize; përcaktimin e kundërmasave të lejuara gjatë një situate emergjence në të cilën sistemet mund të jenë nën sulm; përcaktimin e metodave optimale dhe të zbatueshme për garantimin e sigurisë së informacionit; përcaktimin e metodave testuese për masat e sigurisë dhe veprimet e nevojshme për t'i zbatuar ato; përmirësimin e sistemeve të monitorimit dhe identifikimit të ndërhyrjeve në infrastrukturën kritike në nivel të FA; përcaktimin e kërkesave të sakta të sigurisë në marrëdhënie me siguruesit publik dhe privat të shërbimeve; krijimin dhe fuqizimin e sistemeve rezervë të të dhënave, etj.
- Në vlerësimin dhe përcaktimin përfundimtar të masave për sigurinë në rrjetet kompjuterike, i rëndësishëm është dhe certifikimi i tyre. Akreditimi i rrjeteve dhe sistemeve mbetet një drejtim i rëndësishëm dhe urgjent i punës së strukturave që administrojnë sigurinë në rrjete dhe sisteme. Duhet ndryshuar konceptimi i masave të sigurisë së informacionit nga ai statik në dinamik dhe reagues. Rritja e mundësive të përdorimit të produkteve të certifikuara, për sistemet në pronësi të MM dhe të FA gjithashtu do të ndihmojë në rritjen e besimit dhe përmirësimin e sigurisë së Sistemeve te Ndërlidhjes dhe të Informacionit (SNI) dhe shërbimet që u ofrohen strukturave nëpërmjet këtyre sistemeve.
- Garantimin e besueshmërisë së aseteve dhe proceseve operative brenda vitit 2017, nëpërmjet mënyrës së trajtimit, që karakteri hibrid dhe i ndryshueshëm i procedurave të tenderimit dhe të prokurimit për materialet dhe shërbimet në fushën e Cyber-it të jetë proaktiv.

- Përfitimin nga kërkim-zhvillimi brenda organizmit të mbrojtjes, por edhe hulumtimi shtesë për ndikimin e aseteve kibernetike, si një kapacitet operativ, si edhe për kërcënimin që paraqesin për Forcat e Armatosura; teknikisht, ligjërisht dhe në drejtim të çrregullimit të mundshëm të proceseve. Ndaj MM/FA, duhet të vazhdojë, të lidhet me këto zhvillime në fushën kibernetike, në nivel kombëtar dhe ndërkombëtar, por gjithashtu të kryejë kërkime në mënyrë të pavarur.
- Organizimin e mbrojtjes nëpërmjet rekrutimit, trajnimit dhe mbajtjes së personelit të kualifikuar, të cilët duhet të jenë të aftë të veprojnë në një mjedis ushtarak. Gjithashtu hartimi i politikave dhe trajtimi i personelit, për të marrë edhe për të mbajtur (ruajtur) njohuritë e nevojshme, kompetencat dhe aftësitë organizative brenda sektorit të mbrojtjes. Sigurisht që mund të merren në konsideratë modele të veçanta të karrierës, për të zhvilluar, kultivuar njohuritë dhe ekspertizën në fushën kibernetike, nëpërmjet shkëmbimeve të personelit, promovimit dhe duke bashkëpunuar me organizma dhe shërbime të tjera. Kjo bën të mundur që personeli të fitojë përvojën e duhur dhe në të njëjtën kohë u jep atyre një perspektivë interesante të karrierës.

4. Ruajtja dhe zhvillimi i aftësive të përdoruesve dhe specialistëve për të zbuluar, trajtuar, lajmëruar dhe reaguar ndaj incidenteve që ndodhin në Sistemet e Ndërlidhjes dhe Informacionit.

Ministria e Mbrojtjes dhe FA duhet të jenë në gjendje të vazhdueshme dhe të përgatitur operacionalisht, me qëllim që të parandalojnë, zbulojnë dhe koordinojnë reagimin ndaj incidenteve serioze në sistemet e ndërlidhjes dhe informacionit. Në këtë kontekst, drejtoritë përgjegjëse për sigurinë e informacionit dhe të sistemeve të ndërlidhjes duhet të kenë një bashkëpunim sa më të ngushtë ndërmjet tyre. Ky bashkëpunim duhet të adresojë me qartësi ngjarjet e ndodhura aksidentalisht ose qëllimisht, duke i klasifikuar në teknike, gabimet njerëzore, aksidente ose fatkeqësi të natyrës.

Incidentet në sisteme përfshijnë sulme të drejtuara ndaj infrastrukturës dhe ndaj informacionit të klasifikuar në tërësi. Së bashku, incidente të vogla ose të mëdha në volum, mund të kenë pasoja serioze (si rrjedhje të informacionit zyrtar ose humbje të konfidencialitetit të informacionit).

Strukturat që administrojnë logjikisht dhe fizikisht sistemet e ndërlidhjes dhe informacionit duhet të garantojnë një proces të qartë të trajtimit dhe reagimit ndaj incidenteve dhe sulmeve. Nëpërmjet procedurave të sakta duhet të vendoset se **çfarë** do të trajtohet si incident në sistem, **kush, kujt**, **kur** dhe **si** do të raportohet etj. Zbatimi i këtyre procedurave do të shoqërohet me mekanizmat e nevojshëm të zbulimit të vendosura në sistemet e ndërlidhjes dhe informacionit për të parandaluar, zbuluar, njoftuar dhe menaxhuar incidentet në sisteme.

Fushat ku duhet të përqendrohemi përfshijnë:

- Drejtoritë përgjegjëse duhet të përcaktojnë qartë se kush do të jetë grupi i njoftimit-alarmit me kapacitetet bazë për të koordinuar dhe menaxhuar incidentet në sisteme, të cilat do të mbështesin funksionet kritike të MM dhe FA. Ky ose këto grupe alarmi duhet të strukturohen-përcaktohen në atë mënyrë, që ata të marrin në konsideratë përdorimin, arkitekturën dhe drejtimin e sistemeve të ndërlidhjes dhe informacionit në MM dhe FA.
- Të përcaktohet qartë se **ku** dhe **kush** do të kryejë funksionin për të mbledhur dhe analizuar informacionin e lidhur me incidentet serioze që ndodhin në sistemet e ndërlidhjes dhe informacionit të MM dhe FA. Është e përcaktuar që incidentet e ndodhura në sistemet e klasifikuara raportohen në DSIK, por duhet përcaktuar si do të raportohen incidentet në rrjetet e paklasifikuar, kujt do t'i raportohet, si do të analizohen dhe si do të

bëhet koordinimi me agjencitë kombëtare të fushës (ALCIRT). Për rrjedhojë, është i domosdoshëm përcaktimi i autoriteti i cili do të ketë përgjegjësinë të koordinojë dhe menaxhojë këto incidente, të sigurojë kohë pas kohe informacion dhe udhëzime për grupet përgjegjëse ndaj incidenteve dhe strukturave që administrojnë logjikisht e fizikisht sistemet e ndërlidhjes dhe informacionit.

Përgatitja për të përballuar incidentet si krimi kiberentik, spiunazhi, sabotazhi dhe terrorizmi, duhet të merret në konsideratë me qëllim formimin e kapaciteteve minimale për këtë qëllim. Njoftimi për rënie të sistemeve, humbjen e lidhjes së pjesshme etj, duhet të vlerësohen dhe konsiderohen nga strukturat që i administrojnë në tërë hapsirën e mundshme të mbrojtjes kibernetike..

5. Forcimi i pozicionit të inteligjencës në Hapësirën Kibernetike.

Shpejtësia e rritjes së hapësirës kibernetike dhe e sistemeve të ndërlidhura, ka zgjeruar me të njëjtën masë edhe mundësitë e grumbullimit të informacionit. Duke qenë se hapësira kibernetike ka një nivel të lartë inteligjence është e nevojshme që të kemi një mbrojtje të infrastrukturës dhe të operacioneve që zhvillohen në këtë fushë.

Parësore për strukturat e mbrojtjes është pasqyrimi i qartë i të gjitha sulmeve dhe kërcënimeve kibernetike që mund të ndodhin, nëpërmjet zhvillimit të njohurive të vetë kërcënimit teknik, si edhe pasqyrimit të qartë të parashikimeve të synimeve dhe qëllimeve të kundërshtarëve apo sulmuesve të ndryshëm.

Agjencia e Inteligjencës dhe Sigurisë së Mbrojtjes (AISM) duhet të krijojë një strukturë brenda saj për mbledhjen, analizimin dhe raportimin e informacionit në hapësirën kibernetike brenda vitit 2017, nëpërmjet aftësive dhe kapaciteteve që posedohen, duke ndërprerë apo ndaluar aktivitetet e paligjshme në këtë fushë.

Informacioni i mbledhur do të përdoret për paralajmërime të produkteve (informacione) të inteligjencës, kompozimin e një kornize të qartë të kërcënimeve kibernetike, zhvillimin e mëtejshëm të produktit në përgjithësi dhe kryerjen e aktiviteteve të kundërzbulimit.

Intensifikimi i bashkëpunimit në hapësirën kibernetike nëpërmjet bashkërendimit/ koordinimit të kapaciteteve të inteligjencës kibernetike, si SIGINT (Signal Intelligence) dhe HUMINT (Human Intelligence), apo kapacitete të kundërzbulimit, për të rritur efikasitetin operacional, duke kombinuar të gjitha asetet që janë në dispozicion. Ky objektiv realizohet duke përfshirë të gjithë strukturat si, DAI, J-6, J-2, ASNI, AISM si edhe Sektorë të tjerë të IT-së.

Me anë të këtij bashkëpunimi sigurohet, një faktor inteligjence më efikas dhe më frytdhënës. Kuptohet që, ky efikasitet do të ketë influencën e tij pozitive si brenda hierarkisë në strukturat e mbrojtjes ashtu edhe në Sigurinë Kombëtare.

Një sfidë më komplekse ka të bëjë me zbulimin e sulmeve dhe sulmeve të mbetura në tentativë. Në rast pamundësie të identifikimit të origjinës, autorit dhe objektivi i një sulmi, ku mundësitë për t'u kundërpërgjigjur do të jenë të kufizuara, lind nevoja për përdorimin e të gjitha burimeve të inteligjencës që kemi në dispozicion si edhe zhvillimin e hetimeve të ndryshme për të përmirësuar dhe rritur në mënyrë të ndjeshme mundësitë për të bashkëpunuar me strukturat e menaxhimit të informacionit, me strukturat e sigurisë, duke krijuar kështu një ndihmesë në shërbimet investiguese kriminale. Përveç kësaj, bashkëpunimi intensiv konfidencial kombëtar do të jetë themelor dhe kyç, për mundësinë e përcaktimit sa më të saktë të identitetit të sulmuesit, si edhe marrjen e masave mbrojtëse sa më të efektshme.

6. ***Intensifikimi i bashkëpunimit në nivel kombëtar dhe ndërkombëtar, partneritetit me biznesin e TI për të garantuar siguri dhe qëndrueshmëri në infrastrukturë, në rrjetet kompjuterike, në produktet që merren dhe në shërbimet që ofrohen.***

- ***Kombëtar***

Siguria kibernetike varet nga aftësia e shteteve dhe institucioneve për të mbrojtur hapësirën e tyre kibernetike, si në mënyre kolektive dhe individuale. Hapësira kibernetike është një fushë në të cilën si aktorët privatë dhe publikë, civilë dhe ushtarakë, kombëtarë dhe ndërkombëtarë, duhet të veprojnë në të njëjtën kohë dhe të jenë reciprokisht të varur nga njëri - tjetri. Teknikat e përdorura nga sulmuesit kryesisht janë të ngjashme dhe të dizenjuara për të shfrytëzuar dobësitë e përgjithshme të rrjeteve dhe sistemeve.

Si menaxher i rrjeteve dhe i sistemeve dixhitale të veta, MM/FA, është një partner i rëndësishëm me njohuri dhe kapacitete specifike. Mënyra sesi kapacitetet do të vihen në dispozicion për operacionet kibernetike do të jenë shumë të detajuara.

Prandaj, është i rëndësishëm hartimi i marrëveshjeve me aktorët e tjerë shtetërorë për përfshirjen e aseteve kibernetike të Ministrisë së Mbrojtjes, si pjesë e intensifikimit të politikës së bashkëpunimit civil-ushtarak si dhe për garantimin e Sigurisë Kombëtare. Vendosja e kapaciteteve të mbrojtjes dhe kontributit të tyre, do të ndikojë në përmirësimin e sigurisë dhe rritjen e besueshmërisë së të gjithë hapësirës kibernetike në Shqipëri. Ky objektiv do të realizohet nëpërmjet organizimit të një metode gjithëpërfshirëse duke përcaktuar qartë rolet, detyrat dhe përgjegjësitë, si dhe një konsultimi të përbashkët për mbajtjen në kontroll të sistemeve të ndryshme në nivel kombëtar.

Gjithashtu, në nivel kombëtar merr rëndësi bashkëpunimi me sektorin publik, si universitetet, dhe me sektorin privat në fushën e kërkimit, zhvillimit dhe trajnimit të personelit. Si rezultat i përballjes me sfida të tilla, si buxhetet e kufizuara dhe mungesa e personelit të kualifikuar, realizimi i këtij bashkëpunimi do të jetë efikas në kuadrin e intensifikimit të bashkëpunimit në nivel kombëtar. Duke qenë se organizmat e Mbrojtjes kontribuojnë në Axhendën Kombëtare të Sigurisë dhe si pjesë integrale e politikave të qeverisë lidhur me sektorin privat, prioriteti i dhënë për sigurinë kibernetike nga industria e teknologjisë së lartë, është një hap më tej në kuadrin e bashkëpunimit me ministritë e tjera, ALCIRT dhe sektorin privat.

- ***Ndërkombëtar***

Në nivel ndërkombëtar, objektivi parësor për Ministrinë e Mbrojtjes është bashkëpunim me vendet, që aspirojnë dhe veprojnë në nivele të ngjashme sigurie, zhvillimi i përbashkët i mjeteve, aftësive dhe teknikave, nëpërmjet shkëmbimit të njohurive dhe eksperiencave në këtë fushë brenda vitit 2015.

Vendi ynë është nënshkrues i Memorandumit të Mirëkuptimit për Mbrojtjen Kibernetike ndërmjet NATO CDMB (Cyber Defence Management Board) dhe vendeve anëtare, Mars 2013. Në këtë kuadër është përgatitur dhe një plan veprimi për CDMB (Cyber Defence Management Board) në nivel kombëtar, në të cilin MM, do të mbështetet pas miratimit të kësaj strategjie.

MM do të bashkëpunojë me NATO-n për forcimin e mbrojtjes kibernetike, nëpërmjet kontributit në zhvillimin dhe zbatimin e politikave të NATO-s dhe përmirësimit të mbrojtjes së sistemeve dhe rrjeteve të veta, si dhe ato të aleatëve. Trajnimi i specialistëve mbetet një

drejtim i rëndësishëm për të formuar kapacitetet e nevojshme për mbrojtjen kibernetike. Për këtë do të synohet pjesëmarrja e vijueshme në veprimtaritë që organizon NATO për mbrojtjen kibernetike duke u trajnuar në struktura të mirëfillta si Qendra e Ekselencës për Mbrojtjen Kibernetike apo njohja e përvojave të vendeve të tjera të NATO-s, që kanë ngritur struktura të veçanta për këtë qëllim. Specialistët e trajnuar jashtë vendit do të shfrytëzohen për organizimin e trajnimeve në nivelin e MM/FA.

IV. ROLET DHE PËRGJEGJËSITË PËR IMPLEMENTIMIN

Megjithëse siguria e informacionit është përgjegjësia e parë dhe kryesore e strukturave të caktuara të MM dhe FA, ndjekja dhe zbatimi me sukses i kësaj strategjie kërkon bashkëpunim efektiv midis strukturave përgjegjëse, me agjencitë e tjera kombëtare të fushës dhe të gjithë përdoruesit individual.

Çdo strukturë e MM dhe FA duhet të jetë në një linjë me parimin e përgjegjësisë dhe të sigurojë se prioritetet e strategjisë zbatohen në vijimësi në të gjitha drejtimet. Në këtë kontekst, çdo strukturë përgjegjëse në MM dhe FA duhet të punojë ngushtë me strukturat e tjera të vartësisë, që masat e sigurisë të jenë të koordinuara me të gjithë aktorët.

Drejtoria e Automatizimit dhe Inovacionit dhe Drejtoria J-6 do të jenë përgjegjësit kryesorë për të ndjekur zbatimin e kësaj strategjie dhe duhet të përfshijnë të gjithë aktorët e nevojshëm në sigurinë e informacionit gjatë zhvillimit dhe implementimit të prioriteteve të vendosura në planin e veprimit.

Drejtoritë përgjegjëse në MM dhe SHPFA duhet të qartësojnë kërkesat ligjore dhe rregullatore të përgjithshme që zbatohen në institucion, kush janë zotëruesit kyç të sistemeve të klasifikuara dhe të paklasifikuara dhe të vendosin kërkesa të qarta për menaxhimin, administrimin fizik dhe logjik të sistemeve të ndërlidhjes dhe informacionit.

Agjencia e Sistemeve të Ndërlidhjes dhe të Informacionit (ASNI) dhe degët e ndërlidhjes në Forca duhet të bashkëpunojnë, të vendosin dhe të përcaktojnë kërkesat për vazhdueshmërinë operacionale të sistemeve të cilat janë shumë të rëndësishme për veprimtarinë e MM dhe FA.

Përdoruesit e sistemeve në MM dhe FA duhet të garantohen që të marrin dhe dërgojnë dokumente elektronikisht në mënyrë të sigurtë që konfidencialiteti, integriteti dhe autenticiteti të mos cënohen. Nga ana e tyre përdoruesit duhet të zbatojnë me korrektësi rregullat dhe procedurat për përdorimin e këtyre sistemeve.

Për të vlerësuar realisht gjendjen aktuale për zhvillimin dhe zbatimin e fushave prioritare të strategjisë, duhet kërkuar rregullisht një rifreskim i masave për zbatimin e planit të veprimit.

Përgjegjësia kryesore për sigurinë e sistemeve të komunikimit dhe të informacionit lidhet me zotëruesit e këtyre sistemeve, administratorin logjik dhe fizik të sistemit si dhe me përgjegjësit e menaxhimit të sistemeve. Puna e sigurisë duhet të jetë një veprim i përditshëm, i mbështetur dhe kontrolluar nga çdo strukturë. Kostot e masave për të promovuar siguri të informacionit në sistemet elektronike duhet të jenë proporcionale me riskun e vlerësuar për sistemet e komunikimit e të informacionit në MM dhe FA.

Përfundim:

- Drejtimet dhe shtyllat kryesore ku mbështet Strategjia për Mbrojtjen Kibernetike sigurojnë që Ministria e Mbrojtjes do të jetë në gjendje të veprojë në mënyrë efikase në hapësirën kibernetike.

- Duke investuar në mbrojtjen kibernetike dhe aftësitë operacionale, do të jemi në gjendje të garantojmë sisteme të teknologjisë së lartë për Forcat e Armatosura, që ato të kryejnë me sukses detyrat e tyre.

- Një plan veprimi më i detajuar, i cili do të përshkruajë se si do të ndiqen dhe zbatohen në të ardhmen prioritetet strategjike, objektivat dhe parimet bazë për politikat e sigurisë të sistemeve të ndërlidhjes dhe informacionit, do të botohet i veçantë dhe do të rishikohet kur paraqitet e nevojshme.