REPUBLIKA E SHQIPËRISË
MINISTRIA E MBROJTJES

STRATEGJIA PËR MBROJTJEN KIBERNETIKE 2024-2028

PËRMBAJTJA

PJESA I

KONTEKSTI STRATEGJIK

1. Hyrje.

Me shpejtësinë e ndryshimit të teknologjisë të informacionit dhe komunikimit, ku sasia dhe vlera e informacionit elektronik rritet dita-ditës dhe në kushtet e internetit pa kufij dhe natyrës anonimate, rreziku i sulmeve kibernetike është ngritur në nivele të pa precedentë.

Sulmet agresive kibernetike të vitit 2022 ndaj Shqipërisë, të cilat vunë në rrezik shumë prej sistemeve qeveritare, treguan dhe njëherë rëndësinë e mbrojtjes së infrastrukturës së informacionit. Sistemet e informacionit të MM-së dhe FA-së nuk u prekën nga ky sulm, por kjo nuk është garanci e paprekshmërisë në të ardhmen. Për të adresuar këtë sfidë, Strategjia e Mbrojtjes Kibernetike hartohet me qëllim forcimin e sistemeve tona të sigurisë kibernetike, zbulimit, parandalimit të sulmeve kibernetike dhe përgjigjen e menjëhershme ndaj incidenteve të mundshme.

Që prej vitit 2014 në Ministrinë e Mbrojtjes janë hartuar dhe realizuar tri strategji për mbrojtjen kibernetike për periudha kohore trevjeçare, të cilat kishin si qëllim të siguronin orientime, koherencë dhe fokus, për një qasje gjithëpërfshirëse dhe për të zhvilluar kapacitetet ushtarake në hapësirën kibernetike. Në kuadër të planeve të veprimit, në zbatim të këtyre strategjive, janë bërë përmirësime të ndjeshme në rritjen e aftësive organizative kundrejt kërkesave të sigurisë kibernetike. Është siguruar një qasje gjithëpërfshirëse e strukturave të MM/FA-së, për të pasur një kuptim më të qartë për hapësirën kibernetike dhe dobësitë e saj. Janë rritur kapacitetet operacionale të SNI-ve, në aspekte të ndryshme të sigurisë kibernetike, dhe është rritur ndërgjegjësimi i personelit në lidhje me sigurinë kibernetike. Investimet në zhvillimin e kapaciteteve kibernetike, si dhe ngritja dhe funksionimi i Njësisë Ushtarake të Sigurisë Kibernetike është rezultati i kësaj përpjekje, e cila ka nevojë për përmirësim dhe modernizim të mëtejshëm.

Mbrojtja kibernetike është pjesë e detyrës kryesore të NATO-s, ku fokusi kryesor është mbrojtja e rrjeteve të veta (përfshirë operacionet dhe misionet) dhe rritja e qëndrueshmërisë në të gjithë Aleancën, duke forcuar vazhdimisht aftësitë e saj me edukimin, trajnimin dhe ushtrimet kibernetike. Të gjitha vendet anëtare të NATO-s janë të përkushtuara për të rritur shkëmbimin e informacionit dhe ndihmën e ndërsjellë në parandalimin, zbutjen dhe rikuperimin e sulmeve kibernetike, ku ekipet e reagimit të shpejtë kibernetik të NATO-s janë në gatishmëri për të ndihmuar aleatët, 24 orë në ditë, nëse kërkohet dhe miratohet.

Ky dokument përfshin vizionin, qëllimet dhe objektivat për të adresuar rreziqet kibernetike dhe për të siguruar që sistemet tona kibernetike në MM dhe FA të jenë të përballueshme dhe të rezistueshme ndaj sfidave të kohës së sotme. Ky është një hap i rëndësishëm drejt forcimit të mbrojtjes kibernetike dhe të sigurisë kombëtare.

2. Kuadri ligjor.

Strategjia për Mbrojtjen Kibernetike merr në konsideratë ligjet kryesore që lidhen me sigurinë dhe krimin kibernetik:

1. Ligji nr. 7895, datë 27.01.1995 "Kodi Penal i Republikës së Shqipërisë", i ndryshuar.
2. Ligji nr. 2/2017 "Për sigurinë kibernetike".
3. Ligji nr. 9918, datë 19.05.2008 "Për komunikimet elektronike në RSh", i ndryshuar.
4. Ligji nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale", i ndryshuar.
5. Ligji nr. 10/2023 "Për informacionin e klasifikuar".
6. Ligji nr. 9880, datë 25.02.2008 "Për nënshkrimin elektronik", i ndryshuar.
7. Ligji nr. 107, datë 15.10.2015 "Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar.
8. Ligji nr. 64/2014 për "Pushtetet dhe autoritetet e drejtimit e të komandimit të Forcave të Armatosura të Republikës së Shqipërisë", i ndryshuar.
9. VKM nr. 1084, datë 24.12.2020 "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe planit të veprimit 2020-2025".
10. Dokumenti "NATO Enhanced Cyber Defence Policy" (Samiti i Uellsit, shtator 2014), i cili konsideron mbrojtjen kibernetike si pjesë të detyrave kryesore të Aleancës për mbrojtjen kolektive, duke konfirmuar që në hapësirën kibernetike zbatohet ligji ndërkombëtar.
11. Vendimet e Samitit të Varshavës (qershor 2016), i cili rikonfirmoi mandatin mbrojtës të NATO-s dhe njohu hapësirën kibernetike si një "domain" operacional, në të cilin NATO-ja duhet të mbrojë veten me efektivitet, ashtu siç vepron në ajër, tokë dhe det.
12. Programi i NATO-s "Cyber Defence Pledge", i cili përfshin dakordësinë e vendeve të Aleancës që të zgjerojnë mbrojtjen kibernetike për rrjetet dhe infrastrukturat kombëtare, të cilat konsiderohen si një çështje me prioritet në të cilën çdo vend aleat, në respekt të përgjegjësive të tij, të përmirësojë qëndrueshmërinë dhe aftësinë për t'u përgjigjur shpejt dhe me efektivitet ndaj sulmeve kibernetike. Çdo vend aleat është dhe do të jetë përgjegjës për të mbrojtur rrjetet e tij kombëtare, të cilat janë të nevojshme të jenë të përshtatshme me ato të NATO-s dhe të njëri-tjetrit, si dhe të zgjerohet shkëmbimi i informacionit për mbështetje të përbashkët në parandalimin, zvogëlimin dhe rigjenerimin nga sulmet kibernetike.

3. Vizioni.

Garantimi i hapësirës kibernetike të sigurt në të gjithë aktivitetin e MM-së dhe FA-së, nëpërmjet vendosjes në eficiencë të kapaciteteve për sigurinë kibernetike, përmirësimit dhe zhvillimit të tyre, për të konsoliduar aftësitë mbrojtëse dhe reaguese, rritjes së vetëdijes, profesionalizmit dhe fuqizimit të bashkëpunimit dhe koordinimit me institucionet kombëtare dhe ndërkombëtare.

PJESA II

QËLLIMI DHE OBJEKTIVAT SPECIFIKË

4. Qëllimi.

Qëllimi i Strategjisë së Mbrojtjes Kibernetike të MM/FA-së është mbajtja e një mjedisi elektronik të sigurt, të besueshëm që mbështet sigurinë në MM/FA për funksionimin normal të sistemeve të komunikimit dhe të informacionit në interes të misionit dhe detyrave.

5. Objektivat.

Për plotësimin e vizionit dhe qëllimit të strategjisë, objektivat kryesore janë:

5.1. Garantimi i sigurisë kibernetike nëpërmjet mbrojtjes së infrastrukturës të informacionit, duke fuqizuar mjetet teknologjike.

5.1. 1. Investimet në infrastrukture dhe SKI për të garantuar sigurinë kibernetike.

Për të realizuar investimet në infrastrukturë kërkohet që:

a) të sigurohet që komponentët hardware dhe software që përdoren në përmirësimin e shërbimeve dhe infrastrukturës (SKI-ve) të jenë të besueshëm, të sigurt dhe të garantojnë mbrojtjen e informacionit;
b) të ketë kërkesa të përshtatshme për performancën e sigurisë kibernetike të implementuar në të gjithë zinxhirin, për produktet TIK, të përdorura në MM dhe FA.

5.1.2. Forcimi i aseteve kibernetike gjatë misioneve dhe operacioneve ushtarake

Për realizimin e misionit dhe të detyrave të tyre, Forcat e Armatosura duhet të mbajnë një hapësire kibernetike të besueshme e të sigurt dhe t'i kushtojnë vëmendje të veçantë zbatimit të rregullave të rrepta për sigurinë e informacionit, në të gjitha sistemet dhe format e shkëmbimit të tij dhe gjatë operacionit apo në misione të ndryshme.
Mbrojtja kibernetike dhe lufta elektronike zë një vend të rëndësishëm në komandim-kontroll. Për të mundësuar përdorimin e aseteve digjitale në operacionet ushtarake institucionet e mbrojtjes do të përqendrohen posaçërisht në:

a) vendosjen e aseteve mbrojtëse digjitale gjatë misioneve;
b) zhvillimin e aseteve kibernetike dhe atyre të inteligjencës kibernetike për përdorim taktik, të nevojshme në procesin e vendimmarrjes;

c) zhvillimin e një doktrine ushtarake të mbrojtjes kibernetike;
ç) integrimin e aspekteve kibernetike në procesin e vendimmarrjes operative, para dhe pas operacioneve.

Në operacionet ushtarake, mbrojtja nga sulmet kibernetike është një kapacitet ushtarak për të mbështetur realizimin e misionit.

5.1.3. Modelimi i praktikave më të mira në mbrojtjen e sistemeve të teknologjisë së informacionit në MM/FA.

Në këtë prioritet Ministria e Mbrojtjes dhe Forcat e Armatosura do të zbatojnë një sërë masash, duke u mbështetur në praktikat më të mira për sigurinë dhe mbrojtjen e SKI-ve. Për këtë kërkohet:

a) mjete dhe teknika të specializuara për të zbuluar dobësi që mund të shfrytëzohen nga hakerat;

b) kryerja e rregullt e auditimeve të sigurisë, vlerësimeve të cenueshmërisë, si dhe testimi i depërtimit;

c) qasje më efektive të kriptimit të të dhënave, realizimit të planifikuar të backup-eve dhe vërtetimin me shumë faktorë në sistemet dhe platformat e MM/FA-së;

ç) bashkëpunim ndërmjet të gjitha strukturave të MM/FA-së, të cilat marrin shërbimet e sistemeve nëpërmjet nyjeve të ndërlidhura në sistem dhe palëve të tjera të sigurisë në strukturat e FA-së, për të promovuar siguri efektive, duke u mbështetur në standardet kombëtare të sigurisë dhe ato të NATO-s.

5.2. Zbatimi i politikave dhe standardeve të plota organizative dhe teknike të sigurisë kibernetike.

Për të realizuar këtë objektiv është e domosdoshme që mbrojtja e infrastrukturës kritike dhe të rëndësishme të informacionit për garantimin e shërbimeve bazë, themelore për MM/FA-në, si dhe menaxhimi i aseteve TIK, të bëhet nëpërmjet kontrollit dhe vlerësimit të vijueshëm të masave të sigurisë.

Për këtë kërkohet zbatimi i politikave, udhëzuesve, rregulloreve dhe SOP, si:

a) Udhëzuesi “Politikat për mbrojtjen kibernetike në Ministrinë e Mbrojtjes dhe Forcat e Armatosura”, të miratuar nga ministri i Mbrojtjes, nëpërmjet urdhrit nr. 794, datë 23.05.2023;

b) Rregulloret dhe udhëzimet e sigurisë të nxjerra nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK);
c) Rregullorja e sigurisë dhe udhëzimet e Agjencisë Kombëtare së Shoqërisë së Informacionit (AKSHI);
ç) Rregulloret dhe udhëzimet e institucioneve të NATO-s për mbrojtjen kibernetike;
d) Rregulloret dhe udhëzimet e institucioneve të BE, ENISA (European Union Agency for Cybersecurity);
dh) SOP të hartuara nga çdo njësi TIK në MM/FA.

Për shkaqe të ndryshimeve teknologjike apo organizative, kërkohet rishikimi i politikave, rregulloreve, standardeve dhe procedurave të sigurisë në MM/FA, për të konfirmuar që politikat e sigurisë dhe standardet vijojnë të kenë përputhshmëri me zhvillimet e teknologjisë së informacionit dhe të jenë reflektuar në praktikat më të mira.

5.3. Rritja e eficiencës dhe gatishmërisë për monitorim, analizë, detektim, menaxhim, kundërpërgjigje ndaj incidenteve kibernetike dhe marrje masash.

Për të arritur këtë objektiv duhet një qasje gjithëpërfshirëse që kombinon teknologjinë, proceset dhe personelin e kualifikuar në strukturat përgjegjëse për menaxhimin dhe sigurinë e informacionit në MM dhe FA. Krijimi dhe funksionimi i NJUSK-ut si arritje dhe realizim i objektivave të strategjisë së kaluar ka rol kryesor në mbrojtjen dhe kundërpërgjigjen ndaj incidenteve kibernetike. Për rritjen e eficiencës dhe gatishmërisë kërkohet:

a) monitorim 24/7 të sistemeve të komunikimit dhe të informacionit në lidhje me mjedisin kibernetik;
b) krijimi i një plan reagimi ndaj incidentit që përshkruan rolet, përgjegjësitë dhe procedurat;
c) hartimi dhe zbatimi i planit të menaxhimit të riskut për të adresuar problematikat dhe zgjidhjen e tyre;
ç) rritja e aftësive dhe kapaciteteve njerëzore për përgjigje të koordinuara dhe të vazhdueshme në kohë reale ndaj incidenteve kibernetike;
d) përdorimi i teknologjisë bashkëkohore për të detektuar anomalitë dhe aktivitete të dyshimta në kohë reale, për të analizuar dhe identifikuar kërcënimet e mundshme.
dh) informacion i vazhdueshëm dhe i përditësuar për përdoruesit e sistemeve të MM/FA-së mbi kërcënimet e sigurisë kibernetike, si dhe si të mbrohet më mirë mjedisi i teknologjisë së informacionit.

5.4. Ndërtimi i një mjedisi të sigurt, të edukuar dhe të ndërgjegjësuar personelin e MM/FA-së.

Për të arritur këtë objektiv duhet angazhimi për të kryer aktivitete të edukimit dhe ndërgjegjësimit për të promovuar një kulturë mbi sigurinë kibernetike midis të gjithë përdoruesve të sistemeve dhe të pajisjeve elektronike, pronë e MM/FA-së, por edhe të punonjësve TIK që administrojnë këto sisteme. Koordinimi dhe bashkëpunimi i të gjithë aktorëve është elementi bazë për garantimin e suksesit. Në këtë aspekt ndërmerren një sërë masash, duke përfshirë:

5.4.1. Të edukojë dhe të fuqizojë të gjithë individët në MM/FA me informacion, besim dhe mjete praktike gjatë përdorimit të mjeteve elektronike digjitale.

Për të arritur këtë objektiv duhet angazhimi për të kryer aktivitete të edukimit dhe ndërgjegjësimit për të promovuar një kulturë mbi sigurinë kibernetike midis të gjithë përdoruesve të sistemeve dhe të pajisjeve elektronike, pronë e MM/FA-së. Duhet që:

a) të sigurohet një nivel i mjaftueshëm edukimi, hulumtimi dhe trajnimi që përdoruesit të jenë të vetëdijshëm mbi kërcënimet kibernetike dhe rreziqet e tij;
b) të realizohet trajnimi i përdoruesve të sistemeve për praktikat e sigurta të komunikimit, për rreziqet e punës online, phishing etj.;
c) të njihen me incidentet e fundit dhe mësimet e nxjerra nga to për të rritur ndërgjegjësimin e përgjithshëm mbi sigurinë kibernetike.

5.4.2. Rritja e përgjegjësisë së strukturave TIK të MM/FA-së për sigurinë kibernetike.

Për rritjen e përgjegjësisë të strukturave TIK duhet të zbatohen:

- rregulla dhe procedura të sakta për përgjegjësitë e strukturave;
- format dhe mënyrat e raportimit të sulmeve kibernetike;
- zhvillimi i kapaciteteve dhe strukturave të dedikuara për sigurinë kibernetike;
- koordinimi ndërmjet strukturave për reagimin ndaj sulmeve kibernetike;
- shkëmbimi i informacionit për sigurinë kibernetike;
- angazhimi i strukturave të inteligjencës në hapësirën kibernetike të MM/FA-së.
- trajtimi i mbrojtjes kibernetike në programet e përgatitjes dhe kualifikimit të personelit të MM/FA-së;
- trajnimi i punonjësve TIK në MM/FA për sigurinë kibernetike.

5.5. Rritja e bashkëpunimit kombëtar dhe atë ndërkombëtar, si anëtar i NATO-s, në fushën e sigurisë kibernetike.

5.5.1. Bashkëpunim në MM/FA.

a) të përcaktohen detyrat dhe prioritetet specifike pas analizës dhe vlerësimit të situatës kibernetike në MM/FA;

b) të realizohen të paktën dy takime në vit nga DPAI, J-6, ASNI dhe NJUSK për të analizuar dhe vlerësuar eficiencën dhe gatishmërinë për monitorim, detektim, menaxhim dhe kundërpërgjigje ndaj incidenteve kibernetike.

5.5.2. Bashkëpunim në nivel kombëtar.

Ky objektiv do të realizohet nëpërmjet:

a) bashkëpunimit dhe koordinimit ndërmjet MM/FA-së dhe institucioneve shtetërore AKCESK, AKSHI, Ministria e Brendshme etj., për të garantuar sigurinë në nivel kombëtar në hapësirën kibernetike;
b) bashkëpunimit të ngushtë në administratën shtetërore, duke rritur sigurinë në sistemet TIK në koherencë me zhvillimet dhe trendin e teknologjisë.

5.5.3. Bashkëpunimin ndërkombëtar për rritjen e sigurisë të hapësirës kibernetike.

Rritja e sigurisë së hapësirës kibernetike për vendin tonë kërkon bashkëpunim në nivel rajonal dhe ndërkombëtar dhe për këtë është e domosdoshme:

a) pjesëmarrja në organizmat dhe forumet e sigurisë kibernetike të NATO-s dhe BE-së dhe rritja e bashkëpunimit me to është prioritet;
b) zhvillimi i mekanizmave dhe i procedurave efikase, për bashkëpunim ndërkombëtar, në rast të incidenteve kibernetike, sulmeve dhe krizave, sipas parimeve të vendosura ndërkombëtarisht;
c) pjesëmarrja në stërvitjet e mbrojtjes kibernetike të NATO-s, si “Cyber Coalition Exercise”, “Crysis Management Exercise” etj., me qëllim rritjen e ekspertizës, si dhe marrjen e praktikave më të mira dhe aplikimin e tyre për rritjen e sigurisë kibernetike;
ç) rritja e bashkëpunimit me Qendrën e Ekselencës së NATO-s për Mbrojtjen Kibernetike.

PJESA III

SFIDAT E SIGURISË DHE KONKLUZIONET

6. Sfidat e sigurisë.

Sfidat e sigurisë për Sistemet e Ndërlidhjes dhe Informacionit (SNI) përfshijnë të gjitha nivelet e strukturave të MM/FA-së, 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:

- **Sulmet kibernetike.**

Hapësira kibernetike, të cilën çdo njeri mund ta përdorë pa kufij kohorë dhe gjeografikë, jep në mënyrë asimetrike avantazhe për sulmuesit keqdashës, jo atyre që mbrohen. Sulmuesit në fushën kibernetike janë të ndryshëm dhe vështirësia për t'u identifikuar ua bën punën më të lehtë. Kriminelët kibernetikë (nga hakerat individualë deri në grupet e organizuara kriminale dhe deri në shtete) mund të përdorin avantazhin e metodave për të lëshuar sulme të cilat janë të pagjurmueshme dhe të vështira për t'u eliminuar. Si rezultat i metodave të sofistikuara, zhvillimit të mjeteve teknologjike të sulmeve kibernetike keqdashëse, ato mund të ekzekutohen në kohë shumë të shkurtër. Nga ana tjetër, kërkuesit shkencorë për të identifikuar një sulmues në hapësirën kibernetike mund të shpenzojnë javë të tëra, muaj, deri në vite. Kundërmasat janë gjithmonë të vonuara në raport me zhvillimin e shpejtë të sulmeve. Sponsorizimi i këtyre sulmeve nga shtetet janë kërcënime serioze, gjithnjë e në rritje ndaj sigurisë kombëtare e në veçanti ndaj objektivave ushtarake, të cilat do të jenë gjithnjë e më shumë pikësynim i sulmeve nëpërmjet spiunazhit dhe sabotazhit kibernetik.
Rritja eksponenciale e ndërlidhjeve të internetit ka çuar në një rritje të konsiderueshme të incidenteve të sulmeve kibernetike, shpesh me pasoja katastrofike dhe të rënda. Sulmet janë zgjedhja kryesore për të kryer qëllime të dëmshme në hapësirën kibernetike ose duke shfrytëzuar dobësitë ekzistuese, ose duke përdorur karakteristikat unike të teknologjive në zhvillim. Zhvillimi i mekanizmave më inovativë dhe më efektivë të mbrojtjes nga sulmet është konsideruar si një kërkesë urgjente në komunitetin e sigurisë kibernetike. Për të ndihmuar në arritjen e këtij qëllimi, duhet bërë një përmbledhje e dobësive më të shfrytëzuara në harduerin, softuerin dhe nivelet e rrjeteve ekzistuese.
Siguria kibernetike ka të bëjë me kuptimin e çështjeve përreth sulmeve të ndryshme kibernetike dhe krijimin e strategjive të mbrojtjes (d.m.th. kundërmasat) që ruajnë konfidencialitetin, integritetin dhe disponueshmërinë e çdo teknologjie digjitale dhe informacioni.

- **Komunikimi dhe transmetimi i informacionit.**

Zhvillimi i internetit dhe i sistemeve të reja kompjuterike, telefonave mobile, pajisjeve magazinuese të lëvizshme dhe tabletat, na e kanë lehtësuar shumë procesin e komunikimit dhe transmetimit të informacionit. Na kanë bërë më eficientë në kryerjen e aktiviteteve të punës, por njëkohësisht jemi bërë më shumë të pambrojtur e të ekspozuar ndaj rreziqeve kibernetike në mjedisin ku ushtrojmë detyrat funksionale. Një sfidë e veçantë për shoqëritë e hapura është përdorimi i komunikimit digjital për të ndikuar në mendimin e publikut, për shembull nëpërmjet përpjekjeve të fshehura për të ndikuar në diskutimet mbi mediat sociale dhe duke manipuluar informacionet në portalet e lajmeve. Kjo qasje tashmë ka fituar një rëndësi të veçantë si një element i luftës hibride. Megjithatë avantazhet e metodave të reja të komunikimit dhe mënyrave të përdorimit të sistemeve të informacionit dhe internetit, privatësia personale është gjithashtu e kërcënuar, për shkak të abuzimit me identitetin, e cila është një sfidë në rritje për çdo individ dhe autoritet institucional.

Teknologjitë që kanë rëndësi për forcat ushtarake, kanë rëndësi edhe për jetën civile. Zhvillimet si 5G dhe inteligjenca artificiale (AI), ose aplikimi i tyre praktik në zona si qytetet inteligjente, nuk nxiten nga kërkesat ushtarake, por nga mundësitë që ato ofrojnë për jetën e qytetarëve tanë. Sigurimi i tyre duhet të bëhet në një mënyrë që të jetë në përputhje me përdorimin e tyre në shoqëritë e lira.

- **Ndërgjegjësimi**.

Ndodh që përdoruesit të kenë njohuri minimale të teknologjisë që ata po përdorin dhe teknologjia zbatohet në një mënyrë të tillë që e bën shumë të vështirë vlerësimin e karakteristikave të sigurisë së shumicës së produkteve, në lidhje me mbrojtjen e konfidencialitetit dhe privatësisë së të dhënave të përdoruesit. Që nga fillimi i zhvillimit të teknologjive të komunikimit dhe informacionit deri në ditët e sotme, devijimet në funksionimin e tyre të duhur kanë ndodhur për arsye të ndryshme, nga gabimi njerëzor ose veprimi keqdashës deri të gabimi teknologjik ose mosveprimi organizativ.
Pavarësisht se përdoren teknika të avancuara për ndërgjegjësimin e personelit ndaj rrisqeve kibernetike, një përqindje e mirë e tyre ripërdorin të njëjtat kredenciale ose përdorin kredenciale të dobëta për autentifikim në sisteme, gjë që i bën shumë vulnerabël në vjedhjen e identitetit dhe privatësisë. Përdoruesit duhet të trajnohen ndaj reagimit të metodave phishing që mund të përdorin hakerat, të cilët përdorin aftësitë e tyre të inxhinierisë sociale për të impresionuar ata për vjedhjen e identitetit.

Qëllimi i ndërgjegjësimit të sigurisë kibernetike për personelin e MM-së dhe FA-së është pajisja e punonjësve me njohuritë e nevojshme për të luftuar këto kërcënime. Ata duhet të mësohen mbi kërcënimet e rrezikshme dhe se si të përgjigjen, si dhe procedurat për adresimin e tyre.

Siguria është përgjegjësi e të gjithëve. Edhe sjelljet në dukje të padëmshme ose gabimet e vogla mund të kenë pasoja të mëdha. Ndërgjegjësimi mbi sigurinë ndihmon që të gjithë në një organizatë të marrin masat për zvogëlimin e rreziqeve dhe incidenteve dhe ndihmon të gjithë personelin e MM-së dhe FA-së të mbrojë organizatën dhe veten e tyre.

- **Kufizimet financiare.**

Kufizimet financiare janë sfida më madhore e mundshme. Mbrojtja kibernetike është një prioritet i rëndësishëm në nivel strategjik, ndaj janë të nevojshme investimet në njerëz dhe në teknologji për t'iu përgjigjur sa më mirë riskut aktual.

- **Anonimati.**

Sulmuesit në fushën e sigurisë kibernetike shpeshherë përdorin metoda sulmuese, të cilat janë të vështira për t'u gjurmuar ose për t'u identifikuar, siç janë serverët Proxy, për fshehjen e identitetit të tyre. Një tjetër metodë me efikase e sulmeve kibernetike nga hakerat është fshehja e

identitetit të tyre, nëpërmjet sistemit të një përdoruesi fundor, i cili ka rënë viktimë e sulmit kibernetik.

7. Konkluzione.

Për shkak të ritmit të lartë të ndryshimit të teknologjisë dhe zhvillimeve të shpejta në mjedisin e kërcënimeve të hapësirës kibernetike, është e nevojshme të ndërmerret vlerësim i vazhdueshëm dhe rishikime të rregullta mbi përshtatshmërinë e politikave të sigurisë kibernetike në MM/FA. Qëllimi duhet të jetë përparimi teknologjik, si dhe bashkëpunimi dhe koordinimi me vendet e tjera, në mënyrë që të jemi në gjendje të reagojmë më shpejt se dobësitë dhe kërcënimet. Një hapësirë kibernetike e sigurt na lejon të krijojmë një themel të fortë mbi sfidat e hapësirës komplekse kibernetike.
Për realizimin e vizionit, qëllimit dhe objektivave të kësaj strategjie hartohet "Plani i Veprimit për Zbatimin e Strategjisë së Mbrojtjes Kibernetike për vitet 2024-2028", i cili duhet të mbështetet në parimet bazë të mëposhtme:

- **Përgjegjësi të ndara**- Të gjithë përdoruesit e sistemeve në MM/FA, gjatë shfrytëzimit të përfitimeve nga rrjetet kompjuterike, duhet të ndërmarrin hapa të arsyeshëm për të siguruar sistemet që përdorin, të bëjnë kujdes gjatë komunikimit dhe ruajtjes së informacionit dhe të dhënave, si dhe të kenë një detyrim për të respektuar informacionin dhe sistemet e të tjerëve.
- **Partneritet** - Bazuar në përgjegjësitë e ndara, një përqasje në sigurinë kibernetike, nëpërmjet partneritetit me të gjithë aktorët kombëtarë dhe ndërkombëtarë në fushën e sigurisë kibernetike, është themelore për të pasur sukses.
- **Menaxhimi i rrezikut** - Në një botë të globalizuar në të cilën të gjitha sistemet e lidhura me internetin janë potencialisht të prekshme dhe sulmet kibernetike janë të vështira për t'u zbuluar, nuk ka siguri kibernetike absolute. MM/FA-ja duhet të zbatojnë një përqasje të bazuar në rrezikun ndaj sistemeve për të vlerësuar, vendosur prioritete dhe për të mbështetur burimet e aktiviteteve të sigurisë kibernetike.
- **Mbrojtja e vlerave të Forcave të Armatosura** - MM/FA-ja duhet të ndjekë politika të sigurisë kibernetike që përmirësojnë individin dhe sigurinë kolektive në Forcat e Armatosura, duke ruajtur të drejtën e individëve në MM/FA, për privatësinë dhe vlera të tjera themelore. Ruajtja e këtij ekuilibri është një sfidë e vazhdueshme për të përballuar sfidat komplekse që paraqet siguria kibernetike në MM/FA.

8. Përkufizime.

- **"Siguria kibernetike"** është tërësia e mjeteve ligjore, organizative, teknike dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike.
- **"Abuzimi"** përdoret nga siguria e sistemeve TIK, e cila menaxhon incidentet e sigurisë kompjuterike, si dhe shqyrton ankesat të cilat vijnë për abuzimet në rrjetet kompjuterike.

- **"Ekipi i reagimit emergjent – ComputerEmergencyResponseTeam (CERT)**"është ekip i krijuar për t'iu përgjigjur ndërhyrjeve në rrjet, të cilat synojnë të shkelin sigurinë kompjuterike.
- **"Sulm kibernetik**" do të quajmë një sulm të qëllimshëm në sistemet kompjuterike, si dhe ndërmarrjeve të cilat kanë akses në internet.
- **"Krimi kibernetik**" është përcaktuar si një krim në të cilin një kompjuter është objekt i krimit (hacking, phishing, spamming) ose përdoret si një mjet për të kryer një vepër penale. Kriminelët kibernetikë mund të përdorin teknologjinë kompjuterike për të pasur akses në të dhënat personale ose përdorin internetin për qëllime shfrytëzuese ose keqdashëse.
- **"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.
- **"Incident i sigurisë kibernetike"** është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cenimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit dhe sjell një efekt real negativ.
- **"Infrastrukturë e rëndësishme e informacionit**" është tërësia e rrjeteve dhe sistemeve të informacionit të zotëruara nga një autoritet publik, i cili nuk është pjesë e infrastrukturës kritike të informacionit, por që mund të rrezikojë apo të kufizojë punën e administratës publike në rastin e cenimit të sigurisë së informacionit.
- **"Infrastrukturë kritike e informacionit**" është tërësia e rrjeteve dhe sistemeve të informacionit, cenimi apo shkatërrimi i të cilave do të kishte ndikim serioz në shëndetin, sigurinë dhe/ose mirëqenien ekonomike të qytetarëve dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
- **"Rrezik i sigurisë kibernetike"** është një rrethanë ose një ngjarje e identifikueshme në mënyrë të arsyeshme, e cila mund të shkaktojë cenimin e sigurisë së shërbimeve ose sistemeve të informacionit dhe të rrjeteve të komunikimit.
- **"Spiunazh kibernetik"** është akti i përfshirjes në një sulm ose seri sulmesh në sistemet qeveritare ushtarake apo të biznesit, që lejojnë një përdorues ose përdorues të paautorizuar të shohin apo të marrin materialin e klasifikuar pa lejen e zotëruesit të sistemit.
- **"Sabotazh kibernetik"** janë veprime të qëllimshme dhe keqdashëse që sjellin si pasojë prishjen e proceseve, funksioneve normale të sistemeve apo dëmtimin ose shkatërrimin e pajisjeve apo të informacionit që mbahet në sistemet elektronike digjitale.
- **"Phishing"** është një përpjekje për të aksesuar informacion sensitiv dhe personal, nëpërmjet email-eve, të cilat duket sikur vijnë nga një kompani e besueshme që operon në internet, por në fakt është një website fals, i cili kontrollohet nga persona jo të besueshëm.

- FUND -