STRATEGJIA
PËR
MBROJTJEN
KIBERNETIKE
2018 - 2020

PËRMBLEDHJE

1. HYRJE

Interneti dhe teknologjitë e reja kompjuterike kanë sjellë ndryshime kolosale në ndërkomunikimin e një shoqërie globale. Transformimi i shkaktuar nga ky digjitalizim krijon varësi të reja. Ekonomia, administrata dhe sigurimi i shërbimeve thelbësore tani mbështeten në integritetin e hapësirës kibernetike dhe në infrastrukturën, sistemet dhe të dhënat që e mbështesin atë.

Edhe pse nuk ka gjasa që një konflikt midis shteteve do të kryhet ekskluzivisht në fushën kibernetike dhe të informacioneve, operacionet në fushën kibernetike dhe të informacionit tashmë po luajnë një rol gjithnjë e më të rëndësishëm në konfliktet ushtarake, trend i cili do të rritet në vitet e ardhshme.

Disponibiliteti, integriteti dhe qëndrueshmëria e kësaj infrastrukture janë vazhdimisht duke u përballur me veprime dëmtuese.

Zbulimi ka zëvendësuar mbrojtjen si strategji. Pjesa më e madhe e hardware-ve dhe software-ve, të zhvilluar fillimisht për të lehtësuar këtë mjedis, ka renditur si prioritet efikasitetin, koston dhe komoditetin e përdoruesit, por nuk ka pasur një siguri të projektuar që nga fillimi. Personat keqdashës, organizatat kriminale ose terroriste mund të shfrytëzojnë pikat e dobëta në sistemet e ndërlidhjes dhe komunikimit dhe minimizimi i këtyre pikave është një prioritet kombëtar.

Trendi aktual tregon se incidentet do të vazhdojnë të rriten, për rrjedhojë kostoja për mbrojtjen, si dhe efektet që shkaktojnë sulmet kibernetike do të rriten me shpejt se përfitimet që vijnë nga shërbimet themelore që ofrojnë SNI-të.

Strategjia për Mbrojtjen Kibernetike 2014-2017 e MM-së kishte si qëllim të siguronte orientime, koherencë dhe fokus, për një qasje gjithëpërfshirëse dhe për të zhvilluar kapacitetet ushtarake në hapësirën kibernetike.

Si rezultat i kësaj përshtatjeje, janë bërë përmirësime të ndjeshme në rritjen e aftësive organizative kundrejt kërkesave të sigurisë kibernetike; gradualisht është siguruar një përqasje 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; është rritur ndërgjegjësimi i personelit në lidhje me sigurinë kibernetike.

2. REFERENCA

Strategjia për Mbrojtjen Kibernetike merr në konsideratë:

Dokumentin "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;

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;

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.

Strategjia e Sigurisë Kombëtare 2014-2020 "Për vendosjen dhe respektimin e standardeve më të larta në drejtim të ruajtjes dhe mbrojtjes së informacionit në të gjitha trajtat e ekzistencës së tij, duke përqendruar përpjekje të veçanta për mbrojtjen nga sulmet kibernetike";

VKM nr. 303, datë 31.03.2011 "Për krijimin e njësive të teknologjisë së informacionit e të komunikimit në Ministritë e linjës dhe Institucionet e varësisë";

Ligji nr. 2/2017 "Për Sigurinë Kibernetike".

3. TERMINOLOGJIA

Siguria në hapësirën kibernetike: Një sërë projektesh organizative, ligjore, teknike, fizike dhe arsimore që synojnë sigurimin e funksionimit të pandërprerë të sigurisë 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 – Computer Emergency Response Team (CERT): 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: 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: I referohet botës kompjuterike virtuale dhe më konkretisht është një rrjet i madh kompjuterësh i përbërë nga shumë rrjete kompjuterike në mbarë botën që përdorin protokollin TCP/IP, për të ndihmuar në komunikimin dhe aktivitetet e shkëmbimit të të dhënave.

Terrorizmi kibernetik: Përdorimi i internetit për të kryer veprime të dhunshme që rezultojnë ose kërcënojnë humbje të jetës ose dëmtime të rënda trupore, me qëllim që të arrihen përfitime politike përmes frikësimit. Gjithashtu, konsiderohet një akt terrorizmi në internet ku aktivitetet terroriste, duke përfshirë akte të ndërprerjes së qëllimshme dhe të përhapur të rrjeteve kompjuterike, veçanërisht të kompjuterëve personalë të bashkangjitur në internet me anë të mjeteve të tilla, si viruset kompjuterike, viruset kompjuterike apo skripte të tjera të përdorura me qëllim të keq.

Incident kompjuterik: Është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cenimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit që 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: Konsiderohet sulmi kibernetik që ka si objekt të tij cenimin e konfidencialitetit të një sistemi TIK.

Sabotazh kibernetik: Konsiderohet sulmi kibernetik që ka si objekt të tij cenimin e integritetit dhe disponueshmërisë së një sistemi TIK.

4. VIZIONI

Zhvillimi i aftësive mbrojtëse dhe krijimi i kapaciteteve për sigurinë kibernetike, duke e bërë të besueshme, të qëndrueshme dhe efiçente, fokusuar në të gjitha nivelet strategjike, operacionale dhe taktike të MM-së dhe FA-së, në bashkëpunim dhe koordinim me institucionet kombëtare.

5. QËLLIMI

Qëllimi i Strategjisë së Mbrojtjes Kibernetike është mbajtja e një hapësire kibernetike të besueshme e të sigurt për MM-në dhe Forcat e Armatosura për realizimin e misionit dhe të detyrave të tyre.

Zbatimi i Strategjisë së Mbrojtjes Kibernetike mbështetet në parimet bazë të mëposhtme:

- *Zhvillimi:* Nëpërmjet zhvillimit të qëndrueshëm dhe sistematik të aftësive, teknologjisë së komunikimit dhe informacionit dhe të masave të sigurisë është e mundur të mbrohemi kundër kërcënimeve kibernetike;

- *Përgjegjësisë*: Pakësimi i rreziqeve është i mundur vetëm nëse të gjitha strukturat dhe personeli i MM/FA-së, të përfshira në hapësirën kibernetike, janë të informuar dhe të ndërgjegjësuar për pasojat që rrjedhin nga veprimi ose mosveprimi i tyre në pjesën për sigurinë që u përket atyre dhe në sigurinë e të tjerëve.

- *Bashkëpunimi:* Mbrojtja efektive kundër kërcënimeve në hapësirën kibernetike, e pakufizuar nga ndarje administrative me institucione ose struktura të tjera të shtetit, është e mundur vetëm nëpërmjet bashkëpunimit në nivel kombëtar e ndërkombëtar.

- *Ligji dhe standardet*: Mbrojta kibernetike efektive realizohet nëpërmjet zbatimit rigoroz të përcaktimeve ligjore, politikave, standardeve dhe udhëzimeve përkatëse.

- *Kapacitetet*: Realizimi i mbrojtjes kibernetike efektive arrihet duke pasur burimet e nevojshme njerëzore dhe ato të teknologjisë përkatëse.

- *Strategjitë*: Strategjia e Sigurisë Kombëtare dhe Strategjia Ushtarake i vlerësojnë sulmet kibernetike si kërcënime, rreziqe dhe sfida jokonvencionale.

6. OBJEKTIVAT

- Zbatimi i masave të plota organizative dhe teknike të sigurisë kibernetike në sistemet e komunikimit dhe të informacionit (SKI).
- Rritja e përgjegjësisë së strukturave të MM/FA-së për sigurinë kibernetike.
- Zhvillimi i nivelit dhe aftësive të specialistëve të sigurisë kibernetike dhe të përdoruesve të SKI-ve.
- Rritja e bashkëpunimit me strukturat përgjegjëse në nivel kombëtar dhe në kuadrin e NATO-s.

7. POLITIKAT QË DO TË NDIQEN

1. *Zbatimi i masave të plota organizative dhe teknike të sigurisë kibernetike në Sistemet e Komunikimit dhe të Informacionit (SKI).*
    a. Mbrojtja e infrastrukturës kritike dhe të rëndësishme të informacionit për garantimin e shërbimeve bazë për MM/FA-në;
    b. Menaxhimi i aseteve të teknologjisë së komunikimit dhe informacionit;
    c. Kontrolli i vijueshëm i masave të sigurisë;
    ç. Vlerësimi i vijueshëm i masave të sigurisë;
    d. Reflektimi i kërkesave të sigurisë në projektet e reja të sistemeve të komunikimit dhe informacionit;
    dh. Zbatimi i teknologjive mbrojtëse;

e. Akreditimi i SKI-ve.

2. *Rritja e përgjegjësisë së strukturave të MM/FA-së për sigurinë kibernetike.*
   a. Rregulla dhe procedura të sakta për përgjegjësitë e strukturave;
   b. Format dhe mënyrat e raportimit të sulmeve kibernetike;
   c. Zhvillimi i kapaciteteve dhe strukturave të dedikuara për sigurinë kibernetike;
   ç. Koordinimi ndërmjet strukturave për reagimin ndaj sulmeve kibernetike;
   d. Shkëmbimi i informacionit për sigurinë kibernetike;
   dh. Angazhimi i strukturave të inteligjencës në hapësirën kibernetike të MM/FA-së.

3. *Zhvillimi i nivelit dhe aftësive të specialistëve të sigurisë kibernetike dhe të përdoruesve të SKI-ve.*
   a. Rekrutimi dhe caktimi në detyrë i specialistëve me aftësi të larta për sigurinë e sistemeve të komunikimit dhe informacionit;
   b. Trajnimi i vijueshëm i specialistëve, promovimi dhe certifikimi i tyre;
   c. Konceptimi i trajnimit si një fushë komplekse ku të përfshihet reagimi ndaj incidenteve, testimet penetruese në sisteme, menaxhimi rrezikut, analizat e kërcënimit, mënyrat paralajmëruese;
   ç. Trajtimi i mbrojtjes kibernetike në programet e përgatitjes dhe kualifikimit të personelit të MM/FA-së.

4. *Rritja e bashkëpunimit me strukturat përgjegjëse në nivel kombëtar dhe në kuadrin e NATO-s.*
   a. Bashkëpunimi në bazë të përcaktimeve të Politikës së Sigurisë së Mbrojtjes Kibernetike të Republikës së Shqipërisë;
   b. Detyrimet e ligjit nr. 2/2017 "Për sigurinë kibernetike";
   c. Detyrimet në kuadrin e politikës dhe memorandumit të NATO-s për mbrojtjen kibernetike;
   ç. Pjesëmarrja në trajnimet dhe stërvitjet e NATO-s dhe BE-së për mbrojtjen kibernetike.

8. KOMPONENTËT BAZË MBËSHTETËS TË STRATEGJISË

Zbulimi dhe Parandalimi: Zhvillimi dhe aftësimi i personelit për të identifikuar një sulm kibernetik, nëpërmjet kontrollit dhe masave të sigurisë për të parandaluar një akses të paautorizuar në sistemet e ndërlidhjes dhe informacionit.

Vlerësimi dhe Mbështetja: Nëpërmjet aftësisë për të analizuar dhe për të kuptuar statusin aktual të mbrojtjes kibernetike të SNI-ve dhe kapaciteteve për të mbajtur nivel të përshtatshëm të mbrojtjes kibernetike në kohë.

Përgjigja dhe Rivendosja: E gjendjes për të mbështetur dhe për të zhvilluar aktivitete në lidhje me një ngjarje të zbuluar në sigurinë kibernetike të SNI-ve, për të kufizuar ndikimin e një ndodhie, si dhe zhvillimin dhe implementimin e aktivitete të përshtatshme, për të mirëmbajtur plane për qëndrueshmërinë e SNI-ve dhe për të rivendosur/rigjeneruar çdo kapacitet ose shërbim i cili është ndikuar ose ndërprerë, për shkak të një ndodhie në Sigurinë Kibernetike të sistemeve.

Identifikimi dhe Informimi: Nëpërmjet aftësisë për të menaxhuar informacionin mbi mbrojtjen kibernetike, duke përfshirë grumbullimin, raportimin dhe shkëmbimin, analizën për vlefshmërinë e tij, si dhe kuptimin e rëndësisë së tij, si dhe zhvillimin organizativ për të menaxhuar riskun e sigurisë kibernetike për sistemet, asetet, të dhënat dhe aftësitë.

9. SFIDAT E SIGURISË

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

Rritja e kërcënimeve në hapësirën 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. Si rezultat i metodave të sofistikuara, zhvillimit të mjeteve teknologjike të sulmeve kibernetike ose sponsorizimi i këtyre sulmeve nga shtetet janë kërcënime serioze, gjithnjë e në rritje ndaj sigurisë kombëtare. Për të parandaluar përkeqësimin e mëtejshëm të këtyre kërcënimeve, krijimi "Hapësirës Kibernetike të lirë dhe të ndershme" duhet të jetë paralel me krijimin e "Hapësirës Kibernetike të sigurt";

***Interneti dhe pajisjet mobile*:** Zhvillimi i internetit dhe i sistemeve të reja kompjuterike, sistemet industriale të kontrollit, telefonat mobile, pajisjet magazinuese të lëvizshme (memory stick) dhe tabletat, na bëjnë më shumë efiçent, por edhe më shumë të pambrojtur në mjedisin ku ushtrojmë detyrat funksionale;

Rrjetet sociale dhe portalet: 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;

***Komunikimi dhe transmetimi i informacionit*:** Rrjeti i MM-së dhe FA-së nuk është i mbyllur në një mjedis të kufizuar. Komunikimet elektronike me struktura të tjera të administratës publike, brenda dhe jashtë vendit, përbëjnë një sfidë më vete për shkak të kushteve, rrezikut të dyanshëm, ligjeve e rregullave të ndryshme, të cilat e bëjnë shumë të vështirë që strukturat e MM-së dhe FA-së të ushtrojnë kontroll mbi to;

***Krijimi i marketit të krimit kibernetik*:** Zhvillimi i një marketi të padukshëm, lehtësisht të aksesueshëm, për blerje dhe shitje informacioni, si dhe tregtimin e mjeteve për krimin kibernetik, ka krijuar lehtësira për kriminelët që të shfrytëzojnë këtë mundësi, gjithnjë e më shumë në rritje, për përfitime dhe qëllime keqdashëse.

***Spiunazhi dhe sabotazhi*:** Objektivat ushtarake janë e do të jenë gjithnjë e më shumë pikësynim i sulmeve (hacking) dhe për këtë arsye spiunazhi dhe sabotazhi na bëjnë më ndjeshëm për të rënë pre e sulmeve elektronike ndaj sistemeve të informacionit dhe të komunikimit.

***Privatësia dhe identiteti*:** 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.

***Anonimati dhe atributet*:** Hapësira kibernetike nuk ka kufij fizikë. Sulmuesit në fushën kibernetike janë të ndryshëm dhe vështirësia për t'u identifikuar ua bën punën më të lehtë (nga hakerat individual deri në grupet e organizuara kriminale dhe deri në shtete), p.sh. hakerat dhe kriminelët kibernetikë mund të përdorin avantazhin e metodave për të lëshuar sulme të cilat janë të pagjurmueshme dhe të vështira për t'u eliminuar.

***Asimetria e luftës kibernetike*:** Në 300 milisekonda, një goditje në tastiere mund të udhëtojë dy herë përreth botës por, 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 dhe hakerat gjejnë dobësitë dhe i shfrytëzojnë ato për interes të tyre.

***Kufizimet financiare*:** Kufizimet financiare janë sfida më madhore e mundshme. Duke konsideruar që mbrojtja kibernetike për shumë vende dhe organizata është e vendosur si prioritet në koncept dhe strategji, investimet në "mbrojtjen kibernetike" janë të nevojshme të jenë në nivelin që i korrespondon riskut aktual.

10. MENAXHIMI I RISKUT

Kërcënimet

Kërcënimet kibernetike burojnë nga mundësitë dhe përpjekjet e një kundërshtari për të lëshuar sulm kibernetik mbi SNI-të dhe sistemet ushtarake të armatimit, duke përfshirë sensorët, sistemet e navigimit, të vëzhgimit detar dhe të kontrollit të hapësirës ajrore.

Nisur sa më sipër, në këtë kategori të sulmeve përfshihen:

- *Sabotazhi:* Sulme kibernetike të cilat ndërpresin funksionimin normal të SNI-ve (Sulme të Kundërshtimit të Shërbimit).
- *Spiunazhi:* Sulme kibernetike të cilat përfshijnë ndërhyrje të panjohura nga një palë e tretë ndaj SNI-ve për të lexuar, për të ndryshuar ose të shtojë informacion.

Për shkak të zhvillimit të shpejtë të teknologjisë dhe fushave të përdorimit të saj, në të ardhmen mbrojtja do të përballet me kundërshtime të cilat kanë kapacitete kibernetike sulmuese dhe zbuluese. Këto elemente krijojnë një risk real për konfidencialitetin dhe integritetin e informacionit, si dhe për disponibilitetin e SNI-ve të MM/FA-së dhe sistemeve të tjera të armatimit (përfshirë sensorët, sisteme të navigimit të vëzhgimit detar dhe të kontrollit të hapësirës ajrore).

Dobësitë/shkeljet

Në hapësirën kibernetike (cyber domain) nuk ekziston siguri dhe mbrojtje e plotë. Sidoqoftë, mundësia e një sulmi kibernetik është shumë herë më e madhe se ajo e një sulmi fizik. Eksperienca ka treguar se autoritete të ndryshme dhe mbrojtja kanë qenë viktima të sulmeve kibernetike dhe, për vërtetësinë e këtij konstatimi, do të vijojnë të përballen me sulme kibernetike në të ardhmen, por me sukses të kufizuar.

Ashtu si në territorin e vendit tonë edhe jashtë tij në misione, personeli i mbrojtjes (MM/FA) përdorin internetin (cloud computing), pajisje teknologjike dhe media të lëvizshme (p.sh. thumb drives, USB flash drives etj.). Sfida më e madhe në lidhje me përdorimin e tyre, është ndërgjegjësimi dhe paralajmërimi i personelit që i përdor ato. Shumica e sulmeve kibernetike kanë ndodhur nga gabimet njerëzore, për rrjedhojë "kërcënimet e brendshme" janë reale.

Infrastrukturat kritike të informacionit të MM/FA-së, janë gjithnjë e më shumë objekt i sulmeve kibernetike komplekse. Sulme të tilla ndërmerren posaçërisht ndaj një objektivi të veçantë. Për këtë arsye, MM/FA formojnë "një objektiv të mundshëm" për terroristët ose haker-at, të cilët gjurmojnë për informacion sensitive.

Për shkak të ndikimit të drejtpërdrejt të kufizuar të sulmeve kibernetike, risku i lidhur me to asnjëherë nuk duhet të nënvlerësohet.

Ndikimi

Një analizë e kërcënimeve dhe dobësive do të zbulojë riskun e mundshëm për të cilin ndikimi dhe mundësia mund të jetë kundrejt mjedisit ushtarak të mbrojtjes.

Për këtë shkak, një sulm kibernetik, i cili ndikon në disponibilitetin, konfidencialitetin ose integritetin e SNI-ve të MM/FA-së, mund të ketë një ndikim të madh në funksionimin e institucionit, të strukturave të saj dhe /ose në operacionet ushtarake.

1. Strukturat e Menaxhimit dhe administrimit të SNI-ve të MM/FA-së do të sigurojnë që i gjithë personeli i MM/FA-së mund të punojë në një hapësirë kibernetike të sigurt dhe të mbrojtur.

2. Zhvillimi i kapaciteteve ushtarake të mbrojtjes kibernetike në mbështetje të SNI-ve dhe të veprimeve të FA-së do të lejojë fuqizimin e veprimeve mbrojtëse në SNI dhe në operacione, gjithashtu do të rrisë sigurinë e rrjeteve operacionale dhe të sistemeve ushtarake kundrejt sulmeve digjitale.

3. Me qëllim që të përballohen problemet, si rrjedhojë e kërcënimit kibernetik, dhe mbështetja e strukturave të MM/FA-së, strukturat e SNI-ve do të bashkëpunojnë me aktorët e brendshëm, ALCIRT dhe aktorë të jashtëm, siç është NATO, në përputhje me marrëveshjet e nënshkruara.

Efektet që do të përmbushen:

a. mbajtja e "riskut kibernetik" në një nivel të pranueshëm, për të garantuar zbatimin e misionit ushtarak të mbrojtjes, nëpërmjet analizave të vazhdueshme të kërcënimeve kibernetike, menaxhimit të plotë të dobësive kibernetike dhe mundësitë e implementimit të mjeteve të zbulimit të sulmeve kibernetike dhe reagimit ndaj tyre;

b. kontributi në ruajtjen dhe sigurinë e informacionit për të qenë të aftë të zbatojmë misionet ushtarake me sukses dhe të përmbushim detyrimet ligjore (garantimin e ruajtjes të të dhënave të klasifikuara dhe ato personale);

c. mbrojtja në tërësinë e saj, duhet të jetë e aftë të mbrojë SNI- të dhe sistemet e mirëfillta nga sulmet kibernetike.

11. PRIORITETET

Duke marrë në konsideratë natyrën e veçantë të sigurisë kibernetike, MM/FA do të vijojnë të zhvillojnë kapacitetet e tyre në këtë fushë sipas prioriteteve të mëposhtme:

Prioriteti I: Një sistem përgjigje për mbrojtjen kibernetike.

Identifikimi i shpejtë, shkëmbimi i informacionit dhe rehabilitimi, shpesh mund të zvogëlojë dëmet e shkaktuara nga sulmet kibernetike. Me synim që këto veprime të jenë efektive në mjedisin e punës të MM/FA-së, kërkohet një bashkëveprim midis strukturave përgjegjëse për të kryer analiza, paralajmërime paraprake te përdoruesit dhe koordinimi i përpjekjeve të përbashkëta për të minimizuar dëmet.

MM/FA me synim të jetë e përgatitur për të përballuar një sulm kibernetik, i cili mund të marrë kohë deri në rivendosjen e gjendjes normale të punës të mjeteve kompjuterike, ka nevojë për një plan të

rigjenerimit në rast fatkeqësie nga sulmet kibernetike. Qendrat e ndërlidhjes të kryejnë aktivitete vëzhgimi dhe paralajmërimi.

Prioriteti II: Mbrojtja Kibernetike në MM/FA nëpërmjet programit të zvogëlimit të kërcënimeve dhe dobësive.

Shkeljet e hapësirës kibernetike ndodhin edhe në infrastrukturën kritike të MM/FA-së, duke përfshirë strukturat e varësisë, në strukturat e jashtme mbështetëse (siç janë mekanizmat e internetit) dhe në sitet (vendet) e pasigurta përgjatë lidhjes në rrjetet kompjuterike.

Dobësitë ekzistojnë për një numër shkaqesh, duke përfshirë dobësitë teknologjike, kontroll i dobët për sigurinë gjatë implementimit dhe mungesë të një vëzhgimi të hollësishëm të zbatimit të të gjitha kërkesave të domosdoshme për sigurinë e përdorimit të SNI-ve.

Një program për zvogëlimin e kërcënimeve dhe dobësive të sigurisë kibernetike do të përfshijë përpjekje të përbashkëta të koordinuara, të cilat duhet të kryhen nga strukturat përgjegjëse në MM/FA, në bashkëpunim me sektorët e tjerë qeveritarë dhe ata privatë, për të identifikuar dhe për të rehabilituar dobësitë dhe shkeljet kibernetike serioze përmes aktiviteteve bashkëpunuese. Shkëmbimi i praktikave më të mira, vlerësimi dhe implementimi i teknologjive të reja, komponentë të programit të cilët përfshijnë rritjen e ndërgjegjësimit për sigurinë kibernetike.

Prioriteti III: Vlerësimi i kërcënimeve, dokumentimi, trendi i tyre për të rritur kuptimin mbi konceptin e sigurisë kibernetike.

Vlerësimi i riskut do të dokumentojë kërcënimet dhe trendin e tyre në lidhje me SNI-të e MM/FA-së, si dhe ndikimin kundrejt infrastrukturës kritike dhe shërbimeve themelore.

Përpunimi dhe përshkrimin i tyre do të jetë në mënyrë të tillë për të ndihmuar në rritjen e nivelit të kuptimit të situatës dhe të tregojë kërcënimet dhe risqet ndaj sistemeve TIK.

Prioriteti IV: Program ndërgjegjësimi dhe trajnimi për sigurinë/mbrojtjen kibernetike.

Shumë dobësi në sistemet e informacionit janë për shkak të mungesës së ndërgjegjësimit mbi sigurinë kibernetike për pjesën e përdoruesve të kompjuterëve, administratorëve të sistemit, zyrtarëve të prokurimit, personelit të auditimit të sistemeve, oficerëve të sigurisë të informacionit, oficerëve të sigurisë të SNI-ve dhe INFOSEC. Këto dobësi mund të paraqesin risk serioz kundrejt sistemeve, megjithëse ata mund të mos jenë pjesë e vetë infrastrukturës TIK. Mungesa e personelit të trajnuar vështirëson më tej detyrën për të zvogëluar dobësitë.

Programi i përbashkët i ndërgjegjësimit dhe trajnimit mbi sigurinë kibernetike do të ngrejë nivelin e ndërgjegjësimit të personelit dhe të strukturave të tjera në MM/FA.

Kapacitetet në sigurinë e hapësirës kibernetike do të zhvillohen mbështetur në përputhje me programet e modernizimit të SNI-ve në MM/FA.

12. PËRFUNDIME

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 ata të kryejnë me sukses detyrat e tyre.

Një plan veprimi më i detajuar, i cili do të përshkruajë se si do të ndiqen dhe do të 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 në zbatim të Strategjisë së Mbrojtjes Kibernetike 2018 - 2020.