Ministria e Mbrojtjes
2020

STRATEGJIA PËR MBROJTJEN KIBERNETIKE 2021-2023

PËRMBAJTJA

1. HYRJE.

Sasia dhe vlera e informacionit elektronik rritet dita ditës, sa tashmë jetojmë në një botë të varur nga teknologjia e informacionit dhe komunikimit, e cila mundësohet nga infrastruktura kibernetike e përbërë nga një larmi e madhe teknologjish të ndryshme, të cilat janë në një proces të vazhdueshëm zhvillimi dhe inovacionesh.

Infrastruktura kibernetike po bëhet gjithnjë e më e prekshme, në të njëjtën kohë sulmet kibernetike nga përpjekjet e kriminelëve dhe aktorëve të tjerë me qëllim të keq për të ndërhyrë në sistemet që kontrollojnë mbrojtjen e vendit dhe infrastrukturën kritike, shtohen çdo ditë. Në kushtet e internetit pa kufij dhe natyrës anonimate është gjithnjë e më vështirë të përcaktohet burimi i sulmeve.

Të varur gjithnjë e më shumë nga sistemet komplekse të komunikimit dhe informacionit, NATO-ja dhe vendet partnere duhet të përshtatin dhe të rritin mbrojtjen e tyre në mënyrë që të përballen me sfidat e shfaqura.

Rreziku për sigurinë e sistemeve dhe rrjeteve kompjuterike të MM/FA-së, vlerësohet shumë i lartë, veçanërisht në lidhje me informacionin që trajtohet në këto struktura. Përballja dhe menaxhimi i këtyre rreziqeve duhet të realizohet nëpërmjet bashkëpunimit, koordinimit dhe partneritetit ndërmjet të gjitha palëve të përfshira në fushën e sigurisë kibernetike.

Strategjitë për Mbrojtjen Kibernetike 2014-2020 të MM-së 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.

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.

2. VIZIONI.

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

3. QËLLIMI DHE OBJEKTIVAT.

Qëllimi i Strategjisë së Mbrojtjes Kibernetike të MM/FA-së është mbajtja e një mjedisi elektronik të sigurt, elastik e të besueshëm që mbështet sigurinë në MM/FA dhe rrit përfitimet digjitale në interes të misionit dhe detyrave specifike.

3.1. GARANTIMI I SIGURISË KIBERNETIKE NËPËRMJET MBROJTJES SË INFRASTRUKTURAVE TË INFORMACIONIT, DUKE FUQIZUAR MJETET TEKNOLOGJIKE.

Objektivat:

3.1.1. Zhvillimi i burimeve industriale dhe teknologjike për të garantuar sigurinë kibernetike.

- Të sigurohet që komponentët harduer dhe softuer që përdoren në shërbime dhe infrastruktura kritike të jenë të besueshëm, të sigurt dhe të garantojnë mbrojtjen e të dhënave personale.
- Duhet 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.

3.1.2. Vendosja në eficencë e kapaciteteve të zbulimit, analizës, zvogëlimit dhe masave të kundërpërgjigjes ndaj kërcënimeve kibernetike, duke u fokusuar në infrastrukturën kritike, rrjetet kompjuterike të lidhura me internetin dhe sisteme të tjera në interes të misionit të MM/FA-së.

Ky objektiv përfshin angazhimin e Njësisë Ushtarake të Sigurisë Kibernetike për të ndërtuar kapacitete për mirëmbajtjen e vazhdueshme dhe monitorimin në kohë reale të mjedisit kërcënues, e mbështetur nga plane të vendosura për përgjigje ndaj ngjarjeve që mund të ndodhin.

Ministria e Mbrojtjes dhe Forcat e Armatosura punojnë për vendosjen në efikasitet të kapaciteteve dhe burimeve të Njësisë Ushtarake të Sigurisë Kibernetike për të siguruar:

- monitorim 24/7 të sistemeve në lidhje me mjedisin kibernetik;
- sigurim të kapaciteteve të ndërgjegjësimit për situatën kibernetike dhe koordinim të përgjigjeve ndaj ngjarjeve të sigurisë kibernetike të rëndësishme për sistemet e MM/FA-së;
- aftësinë për të shkëmbyer informacionin dhe të mundësojë përgjigje të koordinuara ndaj incidenteve kibernetike;
- marrjen pjesë aktive dhe lehtësim në shkëmbimin e informacionit me struktura të besuara brenda dhe jashtë vendit, me qëllim për të siguruar dhe mbajtur ndërgjegjësimin për situatën dhe përgjigje të koordinuar për kërcënimet online;
- modelimin e praktikave më të mira në mbrojtjen e sistemeve të teknologjisë së informacionit në MM/FA;
- përgjigje të vazhdueshme dhe në kohë reale ndaj incidenteve kibernetike që mund të ndodhin në rrjetet kompjuterike;
- informacion dhe rekomandime për sigurinë kibernetike për komunitetin e MM/FA-së;
- identifikimin dhe analizimin e sulmeve kibernetike dhe të mbështesë përgjigjet ndaj ngjarjeve kibernetike në sistemet/rrjetet kompjuterike të MM/FA-së;

3.1.3. Forcimi i aseteve kibernetike gjatë misioneve.

Për të mundësuar përdorimin e aseteve digjitale në operacionet ushtarake, në të ardhmen, institucionet e mbrojtjes do të përqendrohen posaçërisht në:

- zhvillimin e mëtejshëm të një doktrine mbrojtëse kibernetike;
- zhvillimin e aseteve ofensive dhe përgatitjen e udhëzimeve për përgatitjen e njësive kibernetike dhe aseteve me një model fleksibël;
- vendosjen e aseteve mbrojtëse digjitale gjatë misioneve;
- zhvillimin e aseteve kibernetike dhe aseteve të inteligjencës kibernetike për përdorim taktik;
- integrimin e aspekteve kibernetike në procesin e vendimmarrjes operative, para dhe pas operacioneve.

3.1.4. Zbatimi i masave të plota organizative dhe teknike të sigurisë kibernetike në Sistemet e Komunikimit dhe të Informacionit (SKI).

Për të realizuar këtë objektiv është i domosdoshëm:

- mbrojtja e infrastrukturës kritike dhe të rëndësishme të informacionit për garantimin e shërbimeve bazë për MM/FA-në;
- menaxhimi i aseteve të teknologjisë së informacionit dhe komunikimit;
- kontrolli dhe vlerësimi i vijueshëm i masave të sigurisë;
- reflektimi i kërkesave të sigurisë në projektet e reja të sistemeve të komunikimit dhe informacionit;
- zbatimi i teknologjive mbrojtëse;
- akreditimi i SKI-ve.

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

Sistemet e komunikimit dhe informacionit në MM/FA dhe informacioni që trajtohet, mbahet apo transmetohet në këto sisteme, janë asete të rëndësishme dhe përfshihen në infrastrukturën kritike kombëtare. Gjithashtu përfshin mbrojtjen e sistemeve të MM/FA-së të ndërlidhura me nyjet e komunikimit dhe sisteme të tjera kombëtare, të cilat janë zhvilluar dhe ndërtuar për të ndihmuar në shpërndarjen e shërbimeve që shkëmbehen ndërmjet MM/FA-së dhe strukturave të tyre të shpërndara në të gjithë territorin e vendit, me struktura të tjera kombëtare ose jashtë vendit.

Në këtë prioritet Ministria e Mbrojtjes dhe Forcat e Armatosura do të zbatojnë një sërë masash, duke përfshirë:

- mundësinë e reduktimit të portave të hyrjes së internetit (internet gateway) në sistemet e MM/FA-së në numrin më të vogël praktik që nevojitet, duke rritur efektivitetin, qëndrueshmërinë dhe sigurinë.
- partneritet 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 në ndërlidhjen e sistemeve të MM/FA-së, duke u mbështetur në standardet kombëtare të sigurisë dhe ato të NATO-s.
- rishikimin e politikave, standardeve dhe procedurave të sigurisë në MM/FA për të siguruar që politikat e sigurisë dhe standardet vijojnë të mbajnë përputhshmëri me zhvillimet e teknologjisë së informacionit dhe reflektohen në praktikat më të mira.

3.2. NDËRTIMI I NJË MJEDISI TË SIGURT, DUKE EDUKUAR DHE NDËRGJEGJËSUAR PERSONELIN E MM/FA-SË.

Trajnimi për ndërgjegjësimin e sigurisë është procesi i ofrimit të edukimit zyrtar të sigurisë kibernetike për personelin e MM/FA-së në lidhje me një sërë kërcënimesh të sigurisë së informacionit dhe politikat dhe procedurat për adresimin e tyre. Një trajnim i tillë mund të marrë një larmi formash dhe temash të ndryshme. Trajnimi dhe programi janë integrale për ndërtimin e një kulture të sigurisë në organizatat moderne, të varura nga bota digjitale.
Misioni i një programi të mirë trajnimi duhet të jetë ofrimi i këshillave koncize, vepruese dhe të paharrueshme, se si të zvogëlohen rreziqet që lidhen me sigurinë kibernetike dhe teknologjinë e informacionit, qofshin ato digjitale apo fizike.

Objektivat:

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

Personeli në strukturat e MM/FA-së përdor sistemet e komunikimit dhe informacionit, si dhe pajisjet elektronike për një larmi qëllimesh me një ritëm gjithnjë e në rritje. Për të mbrojtur dhe siguruar informacionin që ata prodhojnë apo transmetojnë nëpërmjet sistemeve, është thelbësore që përdoruesit e këtyre mjeteve të jenë të vetëdijshëm mbi kërcënimet kibernetike dhe të kuptojnë mjedisin kibernetik dhe rreziqet e tij.

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. Në këtë aspekt ndërmerren një sërë masash, duke përfshirë:

- krijimi i Njësisë Ushtarake të Sigurisë Kibernetike do të sigurojë komunitetin e përdoruesve të sistemeve të MM/FA-së që të ketë akses në informacion mbi kërcënimet e sigurisë kibernetike, dobësitë në sistemet që ata përdorin dhe informacion tjetër se si të mbrojnë më mirë mjedisin e teknologjisë së informacionit;
- Njësia Ushtarake e Sigurisë Kibernetike do të ketë mjetet e duhura të implementuara të raportimit, për të adresuar problemet në rritje në lidhje me viruset etj.;
- strukturat e angazhuara në menaxhimin e sigurisë të mjedisit kibernetik në MM/FA, duhet të gjejnë mundësi të tjera për të informuar më mirë dhe edukojnë

përdoruesit e sistemeve në një shkallë më të gjerë për rreziqet e punës online, duke përfshirë edhe sigurinë kibernetike;

- njohjen e përdoruesve me Autoritetin Kombëtar të Certifikimit Elektronik dhe Sigurisë Kibernetike, si dhe faqen zyrtare të AKCESK-së, në të cilin mund të gjendet informacion mbi kujdesin e përdoruesve të mjeteve elektronike, rekomandime mbi kujdesin ndaj çështjeve të ndryshme kibernetike, blerjet dhe shitjet online, raportimet mbi përmbajtje të paligjshme etj.
- rritje e njohurive dhe ndërgjegjësimit për rrezikun kibernetik në internet. Edukimi dhe trajnimi sigurojnë që njohuritë në fushën e kibernetikës janë të përfshira në të gjitha shtresat e institucionit për të bërë të vetëdijshëm personelin e MM/FA-së për mundësitë dhe rreziqet e botës digjitale. Kjo siguron që mund të zbulohen sulmet në internet dhe të përfshijnë masa mbrojtëse edhe më shpejt;
- të zhvillojë programe për stërvitje/ushtrime mbi sigurinë kibernetike, të testojë dhe të përmirësojë më tej programet e përgjigjes ndaj incidenteve kibernetike;
- të marrë pjesë aktive në stërvitjet që organizon NATO-ja në fushën e sigurisë kibernetike.

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

- 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.

3.2.3. Zhvillimi i nivelit dhe aftësive të specialistëve të sigurisë kibernetike dhe të përdoruesve të SKI-ve.

- rekrutimi dhe caktimi në detyrë i specialistëve me aftësi të larta për sigurinë e sistemeve të komunikimit dhe informacionit;
- trajnimi i vijueshëm i specialistëve, promovimi dhe certifikimi i tyre;
- konceptimi i trajnimit si një fushë komplekse, ku të përfshihet reagimi ndaj incidenteve, testimet penetruese në sisteme, menaxhimi i rrezikut, analizat e kërcënimit, mënyrat paralajmëruese;
- trajtimi i mbrojtjes kibernetike në programet e përgatitjes dhe kualifikimit të personelit të MM/FA-së.

3.3. RRITJA E BASHKËPUNIMIT KOMBËTAR DHE ATË NDËRKOMBËTAR SI ANËTAR I NATO-S NË FUSHËN E SIGURISË KIBERNETIKE

Objektivat:

3.3.1. Koordinimi dhe bashkëpunimi i të gjithë aktorëve kombëtarë, si elementi bazë për garantimin e suksesit.

- Nëpërmjet një bashkëpunimi të ngushtë në administratën shtetërore mund të rritet siguria dhe zhvillimi i TIK në koherencë me zhvillimet dhe trendin e teknologjisë.
- Brenda MM/FA-së të bashkohen përpjekjet e elementeve organizative në një përdorim më efektiv të ekspertizës dhe aseteve.
- Me sektorin tregtar të zhvillohen programe të përbashkëta kërkimore, zhvillim i aftësive dhe bashkëpunim në arsim dhe trajnim.

3.3.2. Bashkëpunimi ndërkombëtar për rritjen e sigurisë të hapësirës kibernetike.

- Vendosja e partneritet efikas me strukturat kombëtare dhe ndërkombëtare për të promovuar sigurinë dhe qëndrueshmërinë e infrastrukturës, rrjeteve kompjuterike dhe shërbimeve digjitale në MM/FA.
- Në cilësinë e vendit anëtar të NATO-s, Shqipëria njeh hapësirën kibernetike si domainin e pestë të luftës, së bashku me tokën, detin, ajrin dhe hapësirën. Hapësira kibernetike paraqet sfida dhe siguria në këtë hapësirë arrihet vetëm duke menduar në nivel global dhe duke punuar ngushtë në nivel ndërkombëtar.
- Me partnerët ndërkombëtarë, NATO-ja mund të mbështesë FA-në në përgatitjen e standardeve të sigurisë për shtetet anëtare, në promovimin e një shkëmbimi më të mirë të informacionit dhe njohurive, si dhe në sigurimin që vendet mund të operojnë më mirë së bashku.

4. 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 eficentë 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.

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 pishing 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 serverat 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.

5. 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 dhe elastike na lejon të krijojmë një themel të fortë mbi sfidat e hapësirës komplekse kibernetike.

Plani i Veprimit për Zbatimin e Strategjisë së Mbrojtjes Kibernetike për vitet 2021-2023 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.

6. 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 – Computer Emergency Response Team (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.

7. 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.

Ligjet kryesore që lidhen me sigurinë dhe krimin kibernetik:

- Ligji nr. 7895, datë 27.01.1995 "Kodi Penal i Republikës së Shqipërisë", i ndryshuar.
- Ligji nr. 2/2017 "Për sigurinë kibernetike".
- Ligji nr. 9918, datë 19.05.2008 "Për komunikimet elektronike në RSh", i ndryshuar.
- Ligji nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale", i ndryshuar.
- Ligji nr. 8457, datë 11.02.1999 "Për informacionin e klasifikuar", i ndryshuar.
- Ligji nr. 9880, datë 25.02.2008 "Për nënshkrimin elektronik", i ndryshuar.
- Ligji nr. 107, datë 15.10.2015 "Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar.