STRATEGJIA KOMBËTARE E SIGURISË KIBERNETIKE E REPUBLIKËS SË MAQEDONISË 2018 - 2022

Versioni 1.2

Korrik, 2018

Përmbajtja

Versioni:

Versioni	Data	Vërejtje
1.0	11.6.2018	Versioni i punës
1.1	3.7.2018	Versioni i skicës me komente të zbatuara nga palët e interesuara
1.2	17.7.2018	Versioni përfundimtar, i miratuar nga Qeveria e Republikës së Maqedonisë

Përmbledhje

Përforcimi i kapaciteteve kombëtare për ballafaqim me kërcënimet kibernetike dhe përmirësimi i sigurisë kibernetike në nivel kombëtar janë me rëndësi parësore për Republikën e Maqedonisë.

Strategjia nacionale për siguri kibernetike e Republikës së Maqedonisë është dokument strategjik që duhet të shërbejë si udhërrëfyes për zhvillim të mjedisit digjital të sigurt, të besueshëm dhe rezistente, të mbështetur nga objekte cilësore, të cilat bazohen në besim dhe bashkëpunim në fushën e sigurisë kibernetike. Ky dokument është i organizuar në shtatë pjesë.

Pjesa e parë e kësaj strategjie është hyrje në problematikën me theks të veçantë në rritjen e varësisë nga shërbimet në hapësirën kibernetike, rritjen e përdorimit të teknologjive të informacionit dhe komunikimit (TIK) dhe ndikimin negativ të sulmeve komplekse kibernetike në funksionimin e sektorit publik dhe privat. Kjo pjesë fokusohet në nevojën e ekzistencës së dokumenteve strategjike që lidhen me forcimin e kapaciteteve kombëtare të sigurisë kibernetike.

Lënda e analizës në **pjesën e dytë** nga kjo strategji janë trendet kibernetike globale dhe lokale, sfidat dhe kërcënimet që janë kyçe në lidhje me funksionimin e hapësirës kibernetike të Republikës së Maqedonisë.

Pjesa e tretë numëron parimet që mbështesin strategjinë:

- Kapacitetet efektive dhe efikase të sigurisë kibernetike,
- Mbrojtja dhe parandalimi,
- Siguria për zhvillimin ekonomik,
- Besimi dhe disponueshmëria dhe
- Siguria juridike.

Në **pjesën e katërt** janë përcaktuar të gjitha palët e interesuara në fushën e sigurisë kibernetike që përfshihen në strategji: sektori publik, sektori privat, bashkësia akademike, qytetarët dhe shoqatat qytetare.

Pjesa e pestë përfshinë vizionin dhe misionin e Strategjisë Kombëtare të Sigurisë Kibernetike të Republikës së Maqedonisë.

Në **pjesën e gjashtë** janë 5C - qëllimet e Strategjisë kombëtare për sigurinë kibernetike. Këto qëllime përcaktohen në drejtim të:

1. Krijimi i infrastrukture TIK rezistente ndaj kërcënimeve kibernetike identifikimi dhe zbatimi i vendimeve të përshtatshme për mbrojtjen e interesave kombëtare.
2. Promovimi i kulturës së sigurisë kibernetike, me qëllim të kuptimit të gjithanshëm të kërcënimeve kibernetike, si dhe ndërtimin dhe përmirësimin e kapaciteteve të nevojshme mbrojtëse.
3. Forcimi i kapaciteteve kombëtare për parandalimin, hetimin dhe reagimin e duhur ndaj krimit kibernetik.

4. Forcimi i kapaciteteve për mbrojtjen e interesave kombëtare dhe reduktimi i rreziqeve aktuale dhe të ardhshme në hapësirën kibernetike.
5. Bashkëpunimi dhe shkëmbimi i informacioneve në nivel kombëtar dhe ndërkombëtar.

Pjesa e shtatë i dedikohet përgjithësimit të Planit të veprimit për zbatimin e Strategjisë kombëtare për sigurinë kibernetike, si dhe në prezantimin e disa prej sfidave për zbatimin e suksesshëm. Në këtë pjesë përcaktohen përgjegjësitë që lidhen me organet e pushtetit, në drejtim të mbështetjes së qëllimeve dhe aktiviteteve të përcaktuara në strategji. Po ashtu, është përcaktuar edhe struktura organizative për koordinimin dhe zbatimin e aktiviteteve të përcaktuara në strategjinë dhe planin e veprimit. Në këtë drejtim, zbatimi me sukses i kësaj strategjie nënkupton ngritjen e një këshilli kombëtar për sigurinë kibernetike dhe të një organi me kapacitete operacionale për sigurinë kibernetike, kompetencat dhe aktivitetet e të cilit përcaktohen më poshtë.

Plani i veprimit, i cili do t'i përmbajë masat dhe aktivitetet për realizimin e qëllimeve të përcaktuara, do të përpilohet në afat prej tre muajsh nga miratimi i kësaj Strategjie nga ana e Qeverisë së Republikës së Maqedonisë.

Strategjia kombëtare e sigurisë kibernetike bazohet në parimet e BE-së (Cybersecurity Strategy of the European Union) dhe NATO-së (NATO Cyber Defence Pledge) dhe organizatave të tjera ndërkombëtare.

Hyrje

Në vitet e fundit, përdorimi i teknologjive të informacionit dhe komunikimit (TIK) ka ardhur vazhdimisht në rritje. Në të njëjtën kohë, ky zgjerim është një shtytës themelor i globalizimit dhe jep një kontribut të rëndësishëm në zhvillimin e ekonomisë, standardin e jetesës dhe mirëqenien në të gjithë shoqërinë.

Përparimi i shpejtë i TIK-ut ofron përfitime të rëndësishme për funksionimin dhe zhvillimin e avancuar të shoqërisë maqedonase. Të gjitha palët e interesuara nga jeta politike, sociale dhe ekonomike në Republikën e Maqedonisë i shfrytëzojnë mundësitë që ofron zgjerimi i madh i TIK-ut. Sipas indekseve globale për zhvillimin e shoqërisë informatike (IDI, NRI, EGDI, GCI), niveli i zhvillimit të Republikës së Maqedonisë në fushën e shoqërisë informatike është në një të tretën statistikore. Ministria e shoqërisë informative dhe administratës dhe institucionet tjera kompetente në vazhdimësi prezantojnë shërbime të reja elektronike me qëllim për të lehtësuar funksionimin e përditshëm të qytetarëve.

Megjithatë, rritja e varësisë nga shërbimet e ofruara në hapësirën kibernetike do të thotë se sistemet jofunksionale të TIK-ut dhe sulmet serioze kibernetike mund të kenë

një ndikim të rëndësishëm negativ në funksionimin e sektorit publik dhe privat, si dhe të shoqërisë në tërësi. Varësia nga teknologjitë e reja dhe nevoja për disponueshmëri më të madhe të shërbimeve në hapësirën kibernetike është arsyeja që përdoruesit dhe institucionet të rrisin ndërgjegjësimin e tyre për rëndësinë e integritetit, autenticitetit dhe besueshmërinë e të dhënave. Rrjetet maqedonase të komunikimit janë pjesë e rrjeteve globale të komunikimit, që do të thotë se incidentet e sigurisë kibernetike diku tjetër mund të ndikojnë në hapësirën dhe shërbimet kibernetike maqedonase, dhe anasjelltas.

Duke marrë parasysh analizat e bëra nga institucionet më relevante botërore në fushën e sigurisë dhe mbrojtjes, nuk ka dyshim se në vitet e fundit kërcënimet kibernetike janë ndër kërcënimet më të rëndësishme të sigurisë për shoqëritë moderne, e cila është arsyeja kryesore për t'i trajtuar ato si pjesë përbërëse e sigurisë kombëtare dhe ndërkombëtare.

Për arsyet e parashtruara, forcimi i kapaciteteve kombëtare për ballafaqim me kërcënimet kibernetike dhe rritja e sigurisë kibernetike janë bërë një nga sfidat kryesore të Republikës së Maqedonisë.

Ekzistenca e dokumenteve strategjike lidhur me këtë sfidë është e një rëndësie vendimtare në përpjekjet për forcimin e kapaciteteve në fushën e sigurisë kibernetike. Zhvillimi i Strategjisë kombëtare për sigurinë kibernetike ka funksionin bazë përmirësimin e kushteve kuadër në këtë fushë. Nevoja për të zhvilluar dhe miratuar një Strategji kombëtare të sigurisë kibernetike lidhet kryesisht me:

1. Aktivitetet, ndërveprimet sociale, ekonomia, si dhe të drejtat dhe liritë themelore të njeriut janë të lidhura ngushtë me aplikimin e TIK-ut, prandaj është e nevojshme të sigurohet hapësirë kibernetike e hapur, e besueshme dhe e sigurt;
2. Përdorimi i sistemeve të TIK dhe zhvillimi i shërbimeve elektronike rrit rrezikun e incidenteve dhe keqpërdorimet kibernetike, gjë që i bën këto kërcënime një nga më seriozet për sigurinë kombëtare;
3. Përcaktimi dhe zhvillimi i politikës së mbrojtjes kibernetike;

4. Vendosja e një qasjeje të integruar, multidisiplinar për të siguruar bashkëpunim dhe koordinim më të ngushtë ndërmjet sektorit të mbrojtjes dhe sigurisë, institucioneve të përfshira në luftën kundër krimit kibernetikë, sektorit privat, qytetarëve dhe organizatave të shoqërisë qytetare, si dhe aktorëve të tjerë përkatës;
5. Forcimi i kapaciteteve operacionale, koordinimi dhe bashkëpunimi ndërmjet institucioneve dhe organizatave përkatëse të përfshira në luftën kundër krimit kibernetikë;
6. Vendosja e standardeve të përbashkëta, trajnimi dhe edukimi i të gjitha institucioneve dhe organizatave të përfshira në zhvillimin e sigurisë kibernetike;
7. Forcimi i kuadrit institucional dhe ligjor në fushën e sigurisë kibernetike.
8. Forcimi i kapaciteteve kombëtare për parandalimin dhe mbrojtjen nga sulmet kibernetike, si dhe zbatimi i aktiviteteve për rritjen e ndërgjegjësimit kombëtar për sigurinë kibernetike.

Strategjia Kombëtare e Sigurisë Kibernetike është zhvilluar në pajtim me Strategjinë e Sigurisë Kibernetike të Bashkimit Europian dhe Politikën dhe Angazhimin e Sigurisë Kibernetike të NATO-së për të siguruar mjedis digjital të sigurt, të sigurt, të besueshëm dhe qëndrueshëm, për të mirën e qytetarëve, bizneset dhe administrata publike.

Trendet kibernetike, sfidat dhe kërcënimet

Rritja e numrit të përdoruesve të internetit dhe TIK-ut dhe rritja e varësisë nga sistemet e TIK-ut

Rritja e numrit të përdoruesve të internetit (në tremujorin e parë të 2017, 73.6% e familjeve kishin qasje në internet në shtëpi) dhe përdoruesit e TIK-ut, së bashku me rritjen e përdorimit të internetit në sektorin e biznesit (duke filluar nga janari 2017, 91.2% e sipërmarrjeve të biznesit me 10 ose më shumë të punësuar kishin lidhje interneti me brez të gjerë) shkakton varësi në rritje nga lidhja globale. Ndërprerje e ofrimit të shërbimeve të caktuara që varen nga TIK, që mund të shkaktojë efekt kaskadë, mund të jetë me rëndësi kritike për funksionimin e shtetit, veçanërisht kur bëhet fjalë për infrastrukturën kritike të informacionit (në tekstin e mëtejmë " KII") dhe sisteme të tjera të rëndësishme të informacionit (në tekstin e mëtejmë "VIS").

Zbatimi i shërbimeve elektronike

Zbatimi i shërbimeve elektronike në Republikën e Maqedonisë do të përmirësojë dukshëm proceset dhe funksionimin e shoqërisë. Megjithatë, duhet pasur parasysh se

shërbimet dhe aplikacionet elektronike do të sjellin edhe sfida të reja dhe rreziqe kibernetike.

Niveli i ulët i sigurisë kibernetike në ndërmarrjet e vogla dhe të mesme

Gjithnjë e më shumë është e nevojshme për ngritje të ndërgjegjës për zbatimin e praktikave më të mira për mbrojtjen e TIK-ut dhe informacionit në ndërmarrjet e vogla dhe të mesme. Të njëjtat shpesh nuk janë në gjendje të përcaktojnë nevojat e tyre për sigurinë kibernetike dhe gjithashtu në shumë raste nuk kanë burime dhe njohuri të mjaftueshme që janë të nevojshme për kalimin e problemeve të regjistruara në këtë fushë. Nga ana tjetër, në raste të caktuara, të dhënat dhe sistemet e këtyre ndërmarrjeve mund të kenë rëndësi kritike për shtetin, veçanërisht nëse ato janë të angazhuara si nënkontraktorë në ndërmarrje dhe institucione më të mëdha.

Rritja e varësisë së sektorit të mbrojtjes dhe të sigurisë nga TIK

Sektorët e mbrojtjes dhe sigurisë janë gjithnjë e më shumë të varur dhe të bazuar në funksionalitetin e sistemeve të TIK-ut. Ndjeshmëria e këtyre teknologjive dhe rreziku i prishjes ose shkatërrimit rritin rreziqet e ndikimit negativ në aftësitë bazë të mbrojtjes dhe sigurisë dhe përmbushjen e kritereve për anëtarësim të plotë në BE dhe NATO.

Krimi kibernetik

Lidhja globale, e cila nëse përdoret siç duhet mund të sigurojë anonimitet të plotë, rrit mundësitë për përdoruesit me qëllim të keq për të hyrë, vjedhur dhe keqpërdorur informacione të ndjeshme. Numër i madh përdoruesish keqdashës dhe organizatash kriminale e kanë njohur hapësirën kibernetike si mundësi për fitim të shpejtë, duke u lejuar atyre një rrezik të reduktuar zbulimi. Globalizimi dhe anonimiteti u mundësojnë përdoruesve keqdashës të kryejnë sulme më të lehta kundër viktimave të përcaktuara më parë, por edhe të kryejnë operacione dhe sulme shumë më të mëdha në një shkallë shumë më të madhe.

Kërcënimet dhe rreziqet që lidhen me përdorimin e rrjeteve sociale

Me rritjen e numrit të rrjeteve sociale, rritja e numrit të përdoruesve të këtyre rrjeteve, si dhe ecuria e algoritmeve të njohjes së fytyrës, janë bazë për rritjen e rrezikut të humbjes së privatësisë, vjedhjes së të dhënave personale, si dhe vjedhjes së identitetit dixhital. Qëllimi i këtyre sulmeve mund të jenë personat fizikë ose juridikë.

Niveli i ulët i ndërgjegjësimit për kërcënimet kibernetike te përdoruesit e fundit

Pjesa e madhe e përdoruesve të internetit në sektorin publik dhe privat, si dhe të gjithë përdoruesit e tjerë, nuk kanë ose kanë një nivel të ulët njohurish për sulmet më të zakonshme kibernetike (si p.sh. phishing, e-shope false, etj.), e cila është arsyeja për një pjesë të madhe të tyre të jenë viktima të një sulmi për të cilin ekzistojnë mekanizma të thjeshtë parandalues dhe mbrojtës.

Nevoja e rritjes për ekspertë të sigurisë kibernetike

Planprogramet ekzistuese në të gjitha nivelet e arsimit (arsimi fillor dhe i mesëm, si dhe të gjitha ciklet e studimeve në universitetet në Republikën e Maqedonisë) nuk i plotësojnë plotësisht nevojat për edukim dhe trajnim të profesionistëve të cilët do t'u përgjigjen sfidave dhe trendeve të fundit në hapësira kibernetike. Nga ana tjetër, nevoja për ekspertë të tillë është gjithnjë në rritje.

Higjiena e pamjaftueshme kibernetike

Një nga arsyet e përhapjes së suksesshme të sulmeve kibernetike është mospërfillja e të ashtuquajturës "higjienë kibernetike" nga përdoruesit dhe organizatat. Sfidë kryesore është se organizatat e kanë shumë të vështirë të vendosin kontroll aktiv mbi higjienën e të punësuarve të tyre dhe në atë mënyrë të korrigjojnë në mënyrë efektive rreziqet e sigurisë kibernetike. Gjithashtu, një nga sfidat është kompleksiteti në rritje i ruajtjes së higjienës bazë kibernetike, si identifikimi i mjeteve të tyre, përditësimi i softuerit, instalimi i arnimeve, menaxhimi i standardeve, edukimi dhe trajnimi i

përdoruesve në organizata më të mëdha. Duke pasur parasysh se shumica e të gjitha kërcënimeve kibernetike parandalohen duke adresuar çështjen e higjienës kibernetike, kjo çështje është një nga çështjet kryesore nga aspekti i sigurisë kibernetike.

Interneti i gjërave

Përderisa numri i pajisjeve të lidhura në internet është rritur ndjeshëm, shumica e përdoruesve injorojnë higjienën e nevojshme kibernetike, përkatësisht mënyrën se si të sillen dhe si të mbrojnë pajisjet që përdorin. Koncepti i "Internetit të gjërave" e përforcon këtë sfidë. Pajisjet elektronike tradicionale, si kompjuterët personalë dhe laptopët, aktivizojnë automatikisht softuerin antivirus, muret e zjarrit, etj., por nuk është e njëjta gjë me pajisjet e tjera inteligjente si TV, frigoriferë, video mbikëqyrje, etj. Për këtë arsye, në periudhën e fundit është vërejtur rritje drastike e abuzimeve online me këto pajisje dhe në të ardhmen kërcënimet nga dhe nga këto pajisje do të jenë dukshëm më të mëdha.

Inteligjenca artificiale

Fusha e inteligjencës artificiale, më saktë të mësuarit me makinë, tashmë ka rol të rëndësishëm në shoqërinë e sotme globale. Zhvillimi i vazhdueshëm në këto fusha ka ndikim pozitiv dhe tashmë po aplikohet për të përmirësuar mekanizmat e sigurisë për t'u mbrojtur nga kërcënimet e ndryshme kibernetike. Nga ana tjetër, inteligjenca artificiale po bëhet nga sfidat kryesore në fushën e sigurisë kibernetike dhe mbrojtjes së privatësisë, sepse e njëjta teknologji përdoret edhe në programet me qëllim të keq.

Rritja e numrit dhe sofistikimit të programeve me qëllim të keq

Në periudhën e fundit jemi përballur me numër në rritje dhe softuer keqdashës gjithnjë e më të sofistikuar. Qindra mijëra softuer të rinj me qëllim të keq prodhohen çdo ditë, dhe në të njëjtën kohë, përdoruesit me qëllim të keq, nëpërmjet mekanizmave të ndryshëm, kufizojnë ndjeshëm opsionet për ndjekjen e burimit të sulmit, përkatësisht inxhinierinë e kundërt dhe analizën mjeko-ligjore. Për më tepër, në vitet e fundit një nga tendencat më të mëdha është rritja e numrit të softuerëve me qëllim të keq të regjistruar që sulmojnë pajisjet celulare. Arsyeja për këtë është se

aplikacionet celulare janë në thelb më të cenueshme dhe se një numër i madh përdoruesish nuk marrin masa themelore të sigurisë për të mbrojtur pajisjet e tyre celulare (si instalimi i softuerit antivirus).

Hardueri dhe softueri i kompromet uar

Numri në rritje i përdoruesve dhe furnizuesve të TIK-ut rrit rrezikun e të ashtuquajturve Sulmet e zinxhirit të furnizimit, ku komponentët e harduerit dhe softuerit komercial të shitur si produkte të disponueshme janë të rrezikuara nga dobësitë e sigurisë, kodi me qëllim të keq ose dyert e pasme të integruara. Vlefshmëria e pamjaftueshme e komponentëve të harduerit dhe softuerit komercial mund të çojë në vjedhje të të dhënave të ndjeshme dhe personale, kibernetike spiunazh ose pjesëmarrja e paqëllimshme në aktivitete me qëllim të keq (për shembull, sulme të bazuara në botnet).

Sasi e madhe e të dhënave (Big data) dhe shërbime *cloud*

Mbrojtja dhe siguria e të dhënave, veçanërisht ato me interes publik (të dhënat relevante për KII dhe VIS) janë thelbësore për Republikën e Maqedonisë. Sasia e të dhënave që përpunohen si në sektorin publik ashtu edhe në atë privat po rritet çdo ditë dhe bashkë me të rritet edhe nevoja për ruajtjen e tyre. Kështu, janë shfaqur forma të reja të ruajtjes së të dhënave, siç është ruajtja në cloud. Megjithatë, përdorimi i shërbimeve online dhe reve kompjuterike mund të çojë në përdorimin e zgjidhjeve joadekuate të sigurisë me besueshmëri të dyshimtë.

Kërcënimet kibernetike ndaj sistemeve të kontrollit industrial dhe infrastrukturës kritike

Duke ndjekur trendet globale, ekziston mundësi reale që në periudhën e ardhshme sektori publik dhe privat të përballen me një numër në rritje të sulmeve kibernetike, duke përfshirë spiunazhin kibernetik industrial, vandalizmin kibernetik dhe identifikimin e dobësive në sektorin e energjisë, sektorin financiar, sektorin e shëndetësisë sistemet e transportit dhe pjesë të tjera të KII dhe VIS. Duke vepruar kështu, mund të pritet një qasje e ndryshme, nga shkaktimi i ndërprerjeve të menjëhershme në funksionimin e pjesëve të infrastrukturës kritike deri te bllokimi i

plotë. Mosfunksionimi i sistemeve të lartpërmendura mund të ketë pasoja fatale, dhe për shkak të heterogjenitetit të lartë të zgjidhjeve teknike, analiza teknike e mëvonshme është dukshëm më e vështirë.

Botnets dhe sulmet DDoS/DoS

"Botnets" përdoren zakonisht për të kryer sulme DDoS/DoS dhe janë gjithnjë e më të fuqishme, elastike dhe të vështira për t'u zbuluar dhe për t'u ndjekur. Zhvillimi në fushën e "interneti i gjërave", të cilat shpesh kanë mekanizma të dobët sigurie, rrisin ndjeshëm hapësirën dhe kapacitetet e sulmit që do të kishin në dispozicion përdoruesit keqdashës.

Ransomware

Numri i aktiviteteve të reja me qëllim të keq të ransomware po rritet në mënyrë eksponenciale, duke sulmuar të gjitha sferat e shoqërisë, përfshirë КИС dhe ВИС. Ky softuerin, edhe pse është i thjeshtë në natyrë, mund të shkaktojë dëme të mëdha duke enkriptuar skedarët ose duke mos qasje në aplikacion ose sistem operativ specifik. Për të fituar qasje në të dhënat e tyre, d.m.th. për të qenë në gjendje të deshifrojnë të dhënat, shumë viktima janë të gatshme të paguajnë një shumë të caktuar për sulmuesit që zhvilluan dhe shpërndanë softuerin keqdashës. Më së shpeshti këto aktivitete ndërmerren nga organizata kriminale që kanë për qëllim të vetëm përfitimin financiar, por në raste të caktuara kanë për detyrë bazë të dëmtojnë sisteme dhe të dhëna të caktuara TIK, pa mundësinë e rikuperimit të të dhënave (NotPetya). Edhe pse ransomware u drejtohet kryesisht individëve, numri i rasteve po rritet gjithnjë e më shumë ku edhe kompanitë dhe institucionet shfaqen si viktima.

Minierat e kriptomonedhave

Abuzimet që lidhen me kriptovalutat janë vjedhje e drejtpërdrejt e të njëjtave nga pronarët e tyre, por edhe vjedhja e burimeve kompjuterike me qëllim që përdoruesit keqdashës të fitojnë një kapacitet më të madh për minimin e kriptomonedhave. Sulmi nuk ka për qëllim vetëm përdoruesit e zakonshëm, por edhe sistemet kompjuterike më

të fuqishme që shpesh janë me rëndësi vitale, të cilat mund të shkaktojnë dëme të konsiderueshme.

Spiunazhi kibernetik

Përqindja në rritje e dixhitalizimit të shoqërisë dhe industrisë çon në shfaqjen e mënyrave të reja nëpërmjet të cilave subjekte ose individë të caktuar mund të kenë qasje të paautorizuar në informacione të ndjeshme ose konfidenciale. Aktivitete të tilla mund të shkaktojnë dëme të mëdha për interesat shtetërore, planet e biznesit dhe reputacionin e kompanive, por edhe të qytetarëve.

Parimet e sigurisë kibernetike

Aftësitë efektive dhe efikase të sigurisë kibernetike

Zhvillimi i madh teknologjik dhe gjithnjë e më shumë zbatimi i arritjeve të reja në TIK u mundëson përdoruesve keqdashës të gjejnë mekanizma të reja për prishjen e sigurisë kibernetike, prandaj është më se e nevojshme që infrastruktura informative-komunikuese në Republikën e Maqedonisë të jetë e gatshme t'u përgjigjet sfidave në hapësirën kibernetike.

Me qëllim për t'iu përgjigjur rreziqeve dhe kërcënimeve të fundit, Republika e Maqedonisë do të mbështesë kërkimin dhe zhvillimin në fushën e sigurisë kibernetike, si dhe edukimin dhe trajnimin në të gjitha nivelet e shoqërisë, duke përfshirë trajnimin e përdoruesve të fundit.

Produkt efektiv i kërkimit dhe zhvillimit në fushën e sigurisë kibernetike mund të arrihet vetëm me bashkëpunim të ngushtë midis të gjithë palëve të interesuara. Prandaj, Republika e Maqedonisë e mbështet plotësisht qasjen shumësektoriale për ndërtimin e kapaciteteve efikase për sigurinë kibernetike.

Për t'u përballur në mënyrë efektive dhe për t'iu përgjigjur në kohë kërcënimeve moderne kibernetike, Republika e Maqedonisë do të mbështesë plotësisht forcimin e

kapaciteteve ekzistuese dhe procedurave për bashkëpunim ndërmjet të gjitha subjekteve apo individëve përkatës në fushën e sigurisë kibernetike.

Mbrojtja dhe parandalimi

Kërcënimet serioze kibernetike për sigurinë e Republikës së Maqedonisë, duke përfshirë operacionet kibernetike dhe spiunazhin e sponsorizuar nga shtete të tjera (përfshirë vjedhjen e pronës intelektuale nga institucionet kritike shtetërore, KII dhe VIS), përdorimi i hapësirës kibernetike për të mbështetur aktivitetet terroriste, trajtohen si rreziqe për sigurinë kombëtare. Një nga parimet kryesore të kësaj strategjie është mbështetja e sistemit për sigurimin e Sigurisë kombëtare të Republikës së Maqedonisë.

Siguria për zhvillimin ekonomik

Zhvillimi i një shoqërie të sigurt dhe aplikimi i të gjitha praktikave dhe proceseve të sigurisë nëpërmjet bashkëpunimit të të gjitha palëve të interesuara do të sigurojë që bizneset të mbeten të besueshme dhe të aksesueshme për klientët, dhe në këtë mënyrë fitimprurëse. Rritja e besimit të qytetarëve në shërbimet dixhitale dhe tregtinë elektronike do të kontribuojë drejtpërdrejt në zhvillimin e ekonomisë dixhitale. Kjo do të kontribuojë që Republika e Maqedonisë të njihet si vend i sigurt për investime dhe operacione afariste.

Zbatimi i zgjidhjeve dhe praktikave më të fundit të TIK-ut dhe lidhja globale do të mbështesë rritjen ekonomike, duke minimizuar eksternalitetet negative si rezultat i incidenteve të sigurisë në hapësirën kibernetike.

Besimi dhe disponueshmëria

Përgjigja ndaj sfidave në hapësirën kibernetike mund të jetë e suksesshme vetëm në rastin e procedurave të mirëndërtuara të bashkëpunimit ndërmjet të gjithë palëve të interesuara që mund të japin kontributin e tyre në fushën e sigurisë kibernetike. Për

këtë arsye nevojitet bashkëpunim i ngushtë ndërmjet sektorit publik, privat dhe atij qytetar.

Mbrojtja e KII dhe VIS është e rëndësisë vendimtare për Republikën e Maqedonisë. Duke pasur parasysh se shumica e kësaj infrastrukture dhe shërbimesh janë në pronësi të sektorit privat, përfshirja e tyre në proceset që lidhen me mbrojtjen e sigurisë kibernetike është thelbësore.

Përkundër të gjitha masave parandaluese për siguri dhe mbrojtje, shfaqja e incidenteve është e pashmangshme, që paraqet rrezik pas disponimit të KII. Aktivitetet e koordinuara në planet e rimëkëmbjes nga fatkeqësitë në KII duhet të rregullohen dhe efektiviteti i tyre duhet të testohet rregullisht nëpërmjet ushtrimeve të përbashkëta kibernetike.

Me qëllim të përmirësimit të bashkëpunimit në fushën e sigurisë kibernetike ndërmjet të gjitha palëve të interesuara, Republika e Maqedonisë do të themelojë Qendër të ekselencës. Kjo Qendër do të synonte shkëmbimin e përvojave ndërmjet sektorit publik, sektorit privat (mbi të gjitha, kompanive që menaxhojnë KII dhe VIS), organizatave të shoqërisë qytetare, akademisë dhe organizatave të tjera.

Siguria juridike

Gjatë zbatimit të masave të sigurisë kibernetike, është e nevojshme të respektohen aktet ligjore pozitive dhe pacenueshmëria e të drejtave themelore të njeriut, parimeve demokratike dhe vlerave themelore. Një nga karakteristikat kryesore të internetit është hapja dhe disponueshmëria e tij për të gjithë, në çdo kohë dhe me një rrjedhë të lirë të garantuar informacioni. Përdoruesit e shërbimeve në hapësirën kibernetike kërkojnë që ajo të jetë i besueshëm dhe t'i sigurojë atyre integritetin e informacionit, lirinë e shprehjes, mbrojtjen e të dhënave personale dhe mbrojtjen e privatësisë. Pritshmëritë e përdoruesve janë që të kenë qasje të lirë në internet pa asnjë ndërhyrje, dëmtim apo ndjekje të paligjshme të komunikimit. Legjislacioni maqedonas, rregulloret europiane, si dhe aktet pozitive ligjore ndërkombëtare në lidhje me të drejtat e njeriut, lirinë e shprehjes dhe mbrojtjen e privatësisë janë universale dhe

janë gjithashtu të zbatueshme në hapësirën kibernetike.

Palët e prekura

Përcaktimi i palëve të interesuara në fushën e sigurisë kibernetike është segment i rëndësishëm që na lejon të përcaktojmë më tej qëllimin e strategjisë.

Strategjia mbulon sektorët e mëposhtëm:

1. **Sektori publik**, në kuptim të kësaj strategjie, janë autoritetet kompetente dhe subjektet e tjera, të cilat në mënyra të ndryshme përfaqësojnë përdoruesit e hapësirës kibernetike dhe subjektet që janë të detyruara të zbatojnë masat që rrjedhin nga strategjia;
2. **Sektori privat,** që është në bashkëpunim të ngushtë me organet kompetente shtetërore dhe rregullatore që janë palë të interesuara të strategjisë, veçanërisht personat juridikë që u nënshtrohen rregulloreve të veçanta për infrastrukturën kritike dhe sistemin e mbrojtjes dhe sigurisë, si dhe me të gjitha subjektet e tjera juridike dhe afariste që përfaqëson në mënyra të ndryshme përdoruesit e hapësirës kibernetike dhe subjektet që janë të detyruara të zbatojnë masat që rrjedhin nga strategjia, me të gjitha veçoritë e atyre subjekteve juridike dhe afariste, për sa i përket fushëveprimit të tyre, numrit i të punësuarve dhe tregjeve që i mbulojnë;

3. **Komuniteti akademik**, institucionet arsimore nga sektori publik dhe privat që në mënyra të ndryshme përfaqësojnë përdoruesit e hapësirës kibernetike dhe subjektet që janë të detyruara të zbatojnë masat që rrjedhin nga strategjia. Në të njëjtën kohë, komuniteti akademik ka një rol në ndërtimin e personelit të përshtatshëm nëpërmjet zhvillimit dhe zbatimit të programeve dhe trajnimeve, si dhe ofrimit të ekspertizës në fushën e sigurisë kibernetike;
4. **Qytetarët dhe organizatat qytetare** që përfshihen përdoruesit e TIK-ut dhe shërbimeve. Gjendja e sigurisë në hapësirën kibernetike prek qytetarët në mënyra të ndryshme. Kjo vlen edhe për qytetarët të cilët

ata nuk përdorin në mënyrë aktive hapësirën kibernetike, por të dhënat e tyre personale ende mund të gjenden atje.

Vizioni dhe misioni

Vizioni

Republika e Maqedonisë të ketë një mjedis digjital të sigurt, të besueshëm dhe elastik, të mbështetur nga objekte të ndërtuara cilësore, ekspertë të kualifikuar, nivel i ndërtuar i besimit dhe bashkëpunim kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike.

Misioni

Republika e Maqedonisë duhet të ketë politika të përcaktuara qartë dhe të qëndrueshme, të cilat do të zbatohen në mënyrë të koordinuar me qëllim të përmirësimit të sigurisë kombëtare kibernetike.

Synimet

Pesë Qëllimet 5C të Strategjisë së sigurisë kibernetike përbëhet nga pesë fusha kyçe dhe synon rritjen e kapaciteteve për t'u mbrojtur nga kërcënimet kibernetike dhe rritjen e sigurisë në hapësirën kibernetike në të gjithë sektorët dhe në të gjitha nivelet.

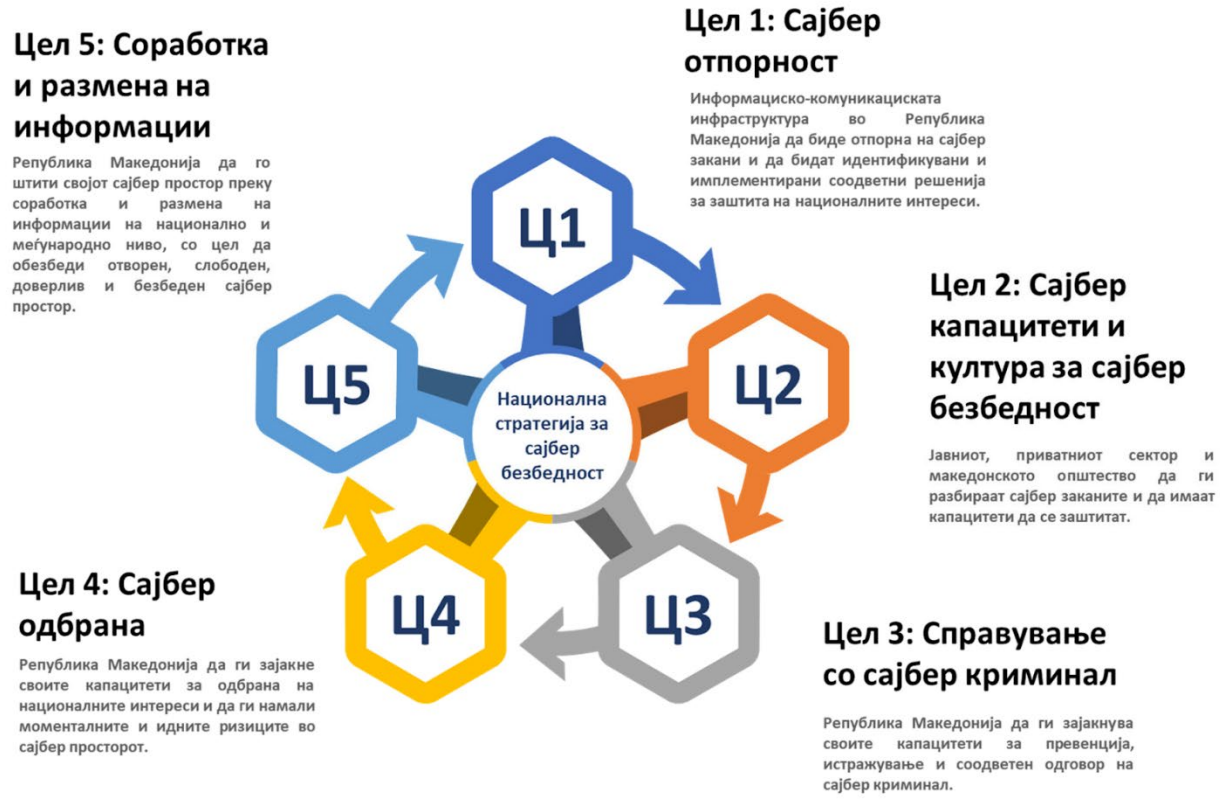

Figura 1: 5C Qëllimet e Strategjisë së Sigurisë Kibernetike

QËLLIMI 1: Rezistenca kibernetike

Infrastruktura informativo-komunikuese në Republikën e Maqedonisë duhet të jetë rezistente ndaj kërcënimeve kibernetike dhe të identifikohen dhe zbatohen vendimet e duhura për mbrojtjen e interesave kombëtare.

Rezistenca kibernetike siguron besueshmëri, integritet dhe disponueshmëri duke identifikuar, mbrojtur dhe parandaluar incidentet kibernetike. Sektori publik dhe privat duhet të kenë informacion dhe propozime në kohë dhe të sakta për të përmirësuar sigurinë kibernetike dhe të jenë në gjendje të bashkëpunojnë me njëri-tjetrin në rast të incidenteve kibernetike. Është e nevojshme të identifikohen të gjitha kapacitetet përkatëse për sigurinë kibernetike midis të gjithë aktorëve dhe duke përcaktuar kompetencat dhe aktivitetet specifike t'i vendosim ato në funksion të përmirësimit të sigurisë kibernetike dhe në funksion të trajtimit të incidenteve kibernetike. Qëllimi është të sigurohet mbrojtja e pjesës më të rëndësishme të infrastrukturës në Republikën e Maqedonisë, përdorimi i zgjidhjeve adekuate për mbrojtjen e interesave shtetërore nga ana e institucioneve kompetente dhe gatishmëria për incidente të rënda (komplekse) kibernetike.

Aktivitetet:

1. Përmirësimi i kapaciteteve dhe aftësive të Qendrës Kombëtare për Reagim ndaj Incidenteve Kompjuterike MKD-CIRT.
2. Identifikimi dhe mbrojtja e KII dhe VIS.
3. Përdorimi i zgjidhjeve më të mira të reagimit ndaj incidenteve kibernetike për të mbrojtur interesat e sigurisë kombëtare.
4. Marrja e masave dhe aktiviteteve për të trajtuar incidentet kibernetike në një shkallë më të gjerë.
5. Zhvillimi i procedurave kombëtare në kohë paqeje, krize, gjendje të jashtëzakonshme dhe luftë për menaxhimin e incidenteve kibernetike që do të mundësojnë bashkëpunim efikas ndërinstitucional, do të përcaktojnë rolin e secilit institucion, të përcaktojnë protokollet dhe procedurat e duhura, si dhe mënyrën e komunikimit, koordinimit dhe shkëmbimin e informacionit.
6. Zhvillimi i metodologjie për vlerësimin e rreziqeve nga kërcënimet kibernetike në nivel kombëtar.

7. Krijimi i kuadrit ligjor unik dhe gjithëpërfshirës për qëndrueshmërinë kibernetike, duke marrë parasysh legjislacionin pozitiv në RM-në dhe BE-në.
8. Ndjekja e vazhdueshme, pranimi dhe zbatimi i standardeve dhe procedurave të njohura ndërkombëtarisht në fushën e sigurisë kibernetike.
9. Mbindërtimi i vazhdueshëm i dokumenteve strategjike kombëtare duke marrë parasysh standardet dhe teknologjitë më të fundit për sigurinë kibernetike dhe kërcënimet kibernetike.
10. Kryerja e analizave të vazhdueshme, kuptimi i gjendjes reale dhe përcaktimi i masave dhe rekomandimeve për ngritjen e nivelit të sigurisë kibernetike në institucionet përgjegjëse për menaxhimin e IKI dhe VIS.
11. Përmirësimi i vazhdueshëm i elasticitetit, integritetit dhe besueshmërisë së KII dhe VIS.
12. Analiza dhe monitorimi i vazhdueshëm i kërcënimeve dhe rreziqeve kibernetike në Republikën e Maqedonisë nëpërmjet sigurimit të rregullt të informacionit nga palët e interesuara.
13. Përcaktimi i procedurave të sakta për ruajtjen dhe mbrojtjen e të dhënave që përpunohen në sistemet KII dhe VIS dhe kryerja e analizave dhe revizionit të vazhdueshëm të efikasitetit të procedurave të përcaktuara.
14. Kryerja e revizioneve të rregullta me qëllim të zbulimit të gabimeve dhe dobësive të sistemeve dhe rrjeteve të informacionit që janë pjesë e IKI dhe VIS.
15. Përmirësimi i vazhdueshëm i nevojave teknologjike dhe organizative për të trajtuar në mënyrë efektive kërcënimet kibernetike.
16. Rritja e kapaciteteve kombëtare për mbrojtje aktive kibernetike dhe marrja e kundërmasave të duhura për t'u përballur dhe për t'iu përgjigjur kërcënimeve kibernetike.

OBJEKTIVI 2: Aftësitë kibernetike dhe kultura e sigurisë kibernetike

Sektori publik, privat dhe shoqëria maqedonase t'i kuptojnë kërcënimet kibernetike dhe të kenë kapacitet për t'u mbrojtur.

Ky synim është më shumë për promovimin e ndërgjegjësimit të kërcënimet kibernetike dhe fokusohet në ndërtimin e kapaciteteve të sigurisë kibernetike midis palëve të interesuara me aktivitete në këtë fushë. Promovimi i kulturës së sigurisë kibernetike nënkupton inkurajimin e përgjegjësisë dhe të kuptuarit e rreziqeve kibernetike në të gjitha sferat e shoqërisë, nëpërmjet zhvillimit të besimit të informuar të përdoruesve në shërbimet elektronike, si dhe përmirësimit të njohurive se si ata mund të mbrojnë të dhënat e tyre personale. Arritja e këtij qëllimi nënkupton krijimin e aftësive, njohurive dhe zgjidhjeve për t'u mbrojtur, duke siguruar qëndrueshmërinë më të madhe ndaj aktiviteteve të dëmshme kibernetike.

Gjithashtu, ky qëllim do të mundësojë shpërndarjen efektive të masave dhe aktiviteteve të sigurisë kibernetike në të gjitha nivelet, duke përfshirë palët e interesuara, për të arritur nivelin e kërkuar të njohurive dhe aftësive të nëpunësve të tyre, përdoruesve dhe palëve të tjera të treta të përfshira në procese. Shkëmbimi i aftësive, njohurive dhe përvojave në fushën e sigurisë kibernetike në nivel kombëtar do të arrihet nëpërmjet krijimit të ekipeve kërkimore ndërdepartamentale ad-hoc të përbëra nga ekspertë të sektorit publik, privat dhe bashkësisë akademike.

Në kontekstin e sigurimit të kapaciteteve adekuate kibernetike, bizneset dhe organizatat të kenë aftësi të përshtatshme kibernetike për t'u përballur me sulmet më të sofistikuara dhe komplekse në hapësirën kibernetike, do të sigurohet një rritje e duhur e ekspertizës në këtë fushë nëpërmjet investimeve në sigurinë kibernetike, e cila është baza për arritjen e performancave konkurrente tregtare.

Aktivitetet:

1. Rritja e kapaciteteve të sigurisë kibernetike në kompanitë e vogla dhe të mesme.
2. Avancimi i kapaciteteve të sigurisë kibernetike në sektorin privat, duke përfshirë infrastrukturën kombëtare, IKI dhe sektorin publik.
3. Zhvillimi dhe promovimi i programeve dhe trajnimeve në fushën e sigurisë kibernetike në të gjitha nivelet.

4. Mbështetja e objekteve kërkimore dhe inovacionit të biznesit nëpërmjet krijimit të qendrës kërkimore shkencore në fushën e sigurisë kibernetike.
5. Pjesëmarrja në projekte dhe aktivitete kërkimore kombëtare dhe ndërkombëtare në lidhje me sigurinë kibernetike.
6. Ofrimi i edukimit dhe trajnimit dhe rritja e ndërgjegjësimit për sigurinë kibernetike në sektorin privat.
7. Sigurimi i udhëzimeve për reagimin në rast të incidenteve kibernetike, krizës kibernetike në të gjitha nivelet e shoqërisë, përfshirë udhëzimet për sjelljen në aktivitetet e përditshme.
8. Kryerja e hulumtimeve dhe përcaktimi i prioriteteve kombëtare dhe, në bazë të tyre, ndërmarrja e aktiviteteve dhe investimeve për zhvillimin e sigurisë kibernetike.
9. Sigurimi dhe zbatimi i zgjidhjeve më të përshtatshme harduerike dhe softuerike për parandalimin, identifikimin dhe menaxhimin e incidenteve kibernetike.
10. Rritja e ndërgjegjësimit dhe njohurive bazë në fushën e sigurisë kibernetike të nxënësve në shkollat fillore dhe të mesme,
11. Përmirësimi i programeve ekzistuese arsimore në shkollat fillore dhe të mesme dhe përfshirja e elementeve nga fusha e sigurisë kibernetike në programet e reja të studimit universitar me qëllim të prodhimit të personelit më të mirë në fushën e sigurisë kibernetike.
12. Rritja e ndërgjegjësimit dhe njohurive bazë në fushën e sigurisë kibernetike te qytetarët dhe organizatat e shoqërisë civile.
13. Sigurimi i edukimit dhe trajnimit adekuat në fushën e sigurisë kibernetike për personelin e administratës publike.
14. Sigurimi i edukimit dhe trajnimit të duhur në fushën e sigurisë kibernetike për personelin menaxherial dhe personelin udhëheqës në sektorin publik dhe privat.
15. Sigurimi i edukimit dhe trajnimit profesional-specialist për personat që punojnë në fushën e sigurisë kibernetike.

16. Krijimi i mekanizmave për mbajtjen e stafit profesional në fushën e TIK-ut dhe sigurisë kibernetike.

QËLLIMI 3: Trajtimi i krimit kibernetik

Republika e Maqedonisë duhet të forcojë kapacitetet e saj për parandalim, hulumtim dhe reagim të duhur ndaj krimit kibernetik.

Zhvillimi dhe përdorimi i teknologjisë së informacionit dhe komunikimit dhe sistemeve të menaxhimit automatik çojnë në shfaqjen e llojeve të ndryshme të abuzimeve të karakterizuara si krim kibernetik. Krimi kibernetik varion nga abuzimi dhe mashtrimi në internet deri te sulmet më të sofistikuara dhe komplekse ndaj sistemeve të informacionit. Krimi kibernetik gjithashtu mund të motivohet dhe kryhet për arsye të ndryshme dhe nga autorë të ndryshëm. Duke pasur parasysh spektrin e gjerë të krimit kibernetik dhe shtrirjen e institucioneve dhe organizatave përkatëse kombëtare përgjegjëse për trajtimin e krimit kibernetik, për këtë qëllim të veçantë është e nevojshme të hartohet një plan i detajuar për trajtimin e krimit kibernetik në nivel kombëtar, i cili do të mbulojë edhe krimin e mundësuar nga hapësirën kibernetike. Ky plan duhet të përcaktojë problemin e krimit kibernetik dhe sfidat që ai gjeneron. Në të është e nevojshme të specifikohen aktivitetet për parandalimin e krimit kibernetik dhe të mundësohet funksionimi më i sigurt i shoqërisë. Një nga metodat më efektive të parandalimit është ofrimi i udhëzimeve dhe zgjidhjeve të përshtatshme për vendosjen ose përmirësimin e higjienës së sigurisë kibernetike në shoqëri në përputhje me praktikat më të mira ndërkombëtare. Një qasje ndërinstitucionale dhe shumëdisiplinore që përfshin të gjitha palët e interesuara është thelbësore për të siguruar një përgjigje efektive ndaj krimit kibernetik.

Aktivitetet:

1. Avancimi i kapaciteteve për trajtimin e krimit kibernetik.

2. Harmonizimi i politikave kombëtare dhe ndërkombëtare lidhur me krimin kibernetik.
3. Krijimi i një kuadri ligjor unik dhe gjithëpërfshirës për krimin kibernetik, duke marrë parasysh legjislacionin pozitiv në Republikën e Moldavisë dhe BE-në.

4. Modernizimi i institucioneve kompetente për luftë efektive kundër krimit kibernetik.
5. Krijimi i procedurave efikase për raportimin dhe hetimin e krimit kibernetik.
6. Krijimi i mekanizmave dhe procedurave formale për bashkëpunim dhe shkëmbim informacioni në fushën e krimit kibernetik ndërmjet subjekteve përkatëse kombëtare dhe shërbimeve të tjera të sigurisë.
7. Promovimi i bashkëpunimit me organizatat rajonale dhe ndërkombëtare për të luftuar krimin kibernetik.
8. Avancimi i mekanizmave ekzistues dhe krijimi i mekanizmave të rinj për bashkëpunim dhe shkëmbim informacioni me sektorin privat dhe civil.
9. Ofrimi i edukimit dhe trajnimit profesional-specialist për personat që punojnë në fushën e identifikimit dhe hetimit të krimit kibernetik.
10. Krijimi i një mjedisi akademik multidisiplinar për të avancuar kapacitetet kombëtare të kërkimit të krimit kibernetik.
11. Pjesëmarrja aktive në krijimin e rregulloreve dhe standardeve ndërkombëtare për krimin kibernetik dhe zbatimin e tyre në nivel kombëtar.
12. Vlerësimi i vazhdueshëm i përshtatshmërisë dhe efektivitetit të rregullores kombëtare të krimit kibernetik.
13. Edukimi i vazhdueshëm i autoriteteve gjyqësore në fushën e sigurisë kibernetike, krimit kibernetik dhe provave elektronike.

QËLLIMI 4: Mbrojtja kibernetike

Republika e Maqedonisë duhet të forcojë kapacitetet e saj për mbrojtjen e interesave kombëtare dhe të zvogëlojë rreziqet aktuale dhe të ardhshme në hapësirën kibernetike.

Me qëllim të përballimit efektiv të rreziqeve në hapësirën kibernetike, Republika e Maqedonisë përcakton kapacitetet për mbrojtje kibernetike sipas standardeve më të larta, si pjesë përbërëse e kornizës kombëtare për sigurinë kibernetike. Zhvillimi i aftësive të mbrojtjes kibernetike në Armatën e Republikës së Maqedonisë është pjesë e mbrojtjes së përgjithshme kombëtare në vend. Kjo sigurohet nga përfshirja e ekspertëve nga sektori i mbrojtjes dhe sigurisë në të gjitha grupet dhe organet e punës për t'u marrë me kërcënimet kibernetike.

Një nga kushtet për vendosjen e një mbrojtjeje efektive kombëtare kibernetike është që të gjitha organizatat që ofrojnë shërbime në hapësirën kibernetike të harmonizojnë vazhdimisht planet operative për mbrojtje nga kërcënimet kibernetike në përputhje me skenarët kombëtarë, me qëllim mbrojtjen e IKI dhe VII.

Bashkëpunimi civilo-ushtarak në nivel ndërkombëtar bazohet në burimet në dispozicion të shtetit dhe të cilat funksionojnë në përputhje me hapësirën kibernetike - në drejtim të paralajmërimit, parandalimit, mbrojtjes, parandalimit, zbulimit dhe mbrojtjes aktive.

Republika e Maqedonisë, si vend partner dhe kandidat për anëtarësim në NATO, Bashkimin Europian dhe organizata të tjera ndërkombëtare ushtarake dhe civile, për të marrë pjesë në mbrojtjen kolektive, është e nevojshme të respektohen plotësisht standardet dhe udhëzimet e këtyre organizatave. dhe të shfrytëzojë burimet dhe mundësitë e ofruara nga këto organizata për zhvillimin dhe zbatimin e kapaciteteve, standardeve dhe trajnimeve të përbashkëta të sigurisë kibernetike. Në sistemet e mbrojtjes kolektive, Republika e Maqedonisë do të bashkëpunojë dhe shkëmbejë informacione me këto organizata në fushën e mbrojtjes kibernetike.

Aktivitetet:

1. Përcaktimi i aftësive kombëtare të mbrojtjes kibernetike.
2. Përcaktimi i aftësive ushtarake në Ministrinë e Mbrojtjes dhe Ushtrinë për të përballuar kërcënimet në hapësirën kibernetike.
3. Formimi, zhvillimi dhe mirëmbajtja e kapaciteteve dhe aftësive të përcaktuara për mbrojtjen kibernetike.
4. Krijimi i një sistemi për mbrojtjen kibernetike të infrastrukturës kritike kombëtare.
5. Krijimi i një kuadri ligjor unik dhe gjithëpërfshirës për mbrojtjen kibernetike, duke marrë parasysh legjislacionin pozitiv në Republikën e Moldavisë dhe direktivat nga NATO dhe BE.
6. Mbrojtja dhe reduktimi i rreziqeve në hapësirën kibernetike.
7. Krijimi dhe ruajtja e bashkëpunimit të ndërsjellë ndërkombëtar për të penguar kërcënimet e përbashkëta kibernetike dhe për të rritur sigurinë dhe stabilitetin kombëtar dhe ndërkombëtar.
8. Përcaktimi dhe bashkërendimi i planifikimit ushtarak për mënyrën dhe përdorimin e aftësive kibernetike ushtarake me mbrojtjen kibernetike kombëtare në situata të ndryshme.
9. Përfshirja dhe kontributi në mbrojtjen kolektive kibernetike nëpërmjet bashkëpunimit ndërkombëtar.
10. Edukimi i vazhdueshëm për të siguruar një nivel të lartë ndërgjegjësimi dhe përgjegjësie personale në lidhje me mbrojtjen kibernetike dhe mbrojtjen dhe sigurinë kombëtare.
11. Zhvillimi dhe zbatimi i një sistemi dhe programesh për shkëmbimin dhe shkëmbimin e informacionit, njohurive dhe përvojave ndërmjet sektorëve publikë, privatë dhe të mbrojtjes-sigurisë në fushën e mbrojtjes kibernetike, me qëllim të mbrojtjes së IKI dhe VII.

OBJEKTIVI 5: Bashkëpunimi dhe shkëmbimi i informacionit

Republika e Maqedonisë e mbron hapësirën e saj kibernetike nëpërmjet bashkëpunimit dhe shkëmbimit të informacioneve në nivel kombëtar dhe ndërkombëtar, me qëllim të sigurimit të hapësirës kibernetike të hapur, të lirë, konfidenciale dhe të sigurt.

Çdo organizatë dhe individ duhet të kujdeset në mënyrë të pavarur për mënyrën dhe përgjegjësinë në përdorimin e teknologjive më të fundit. Megjithatë, nëse duam të kemi një hapësirë të sigurt kibernetike në nivel kombëtar, është e nevojshme të përcaktohen procedura efikase dhe efektive për bashkëpunim dhe shkëmbim informacioni ndërmjet të gjithë aktorëve. Në këtë mënyrë do të mundësohej një mënyrë transparente dhe e sigurt e përdorimit të TIK-ut. Për këtë arsye, është e nevojshme të forcohen kapacitetet, procedurat dhe proceset ndërmjet palëve të interesuara nëpërmjet bashkëpunimit të vazhdueshëm.

Bashkëpunimi ndërkombëtar është një nga segmentet kyç në përpjekjet për rritjen e kapaciteteve për përballimin e kërcënimeve në hapësirën kibernetike. Në një numër të madh të rasteve, Republika e Maqedonisë do të përballej me sulme kibernetike të cilat pjesërisht ose plotësisht janë të organizuara dhe të kryera nga përdorues keqdashës që janë jashtë kufijve fizikë të vendit tonë. Në këtë rast, suksesi i masave të marra për reduktimin e efekteve të incidenteve kibernetike të regjistruara dhe gjetjen dhe marrjen e masave të duhura ndaj autorëve të krimit në thelb varet nga bashkëpunimi i vendosur në nivel dypalësh, rajonal dhe ndërkombëtar. Për të siguruar funksionimin e plotë të institucioneve shtetërore dhe autoriteteve kompetente përgjegjëse për trajtimin e rreziqeve dhe incidenteve në hapësirën kibernetike, nevojiten partneritete ndërkombëtare të këtyre institucioneve me shtete dhe organizata të tjera. Republika e Maqedonisë duhet të marrë të gjitha masat e nevojshme për t'u njohur si një vend që kujdeset për sigurinë në hapësirën e vet kibernetike dhe që dëshiron të përfshihet aktivisht në luftën globale për t'u përballur me abuzimin masiv të hapësirës kibernetike nga përdoruesit keqdashës. Pjesëmarrja aktive ndërkombëtare në përballje

me sfidën globale të kërcënimeve kibernetike do të kontribuojë në rritjen e kapaciteteve shtetërore për përballimin e rreziqeve kibernetike.

Aktivitetet:

1. Promovimi i menaxhimit të internetit dhe normave të sjelljes shtetërore që pasqyrojnë interesat e Republikës së Maqedonisë.
2. Zhvillimi i një modeli efektiv të bashkëpunimit në nivel kombëtar ndërmjet institucioneve që kanë kompetencë në fushën e sigurisë kibernetike dhe përmirësimi i strukturës dhe proceseve ekzistuese të tyre.
3. Zhvillimi i rrjeteve ekzistuese dhe ndërtimi i rrjeteve të reja të bashkëpunimit operacional kombëtar, dypalësh, rajonal, ndërkombëtar.
4. Pjesëmarrja aktive dhe kontributi në aftësinë ndërkombëtare të sigurisë kibernetike dhe ndërtimin e besimit.
5. Shkëmbim efikas i informacionit ndërmjet shtetit dhe subjekteve që menaxhojnë IKI dhe VIS.
6. Mbështetje në shfrytëzimin e mundësive ekonomike të hapësirës kibernetike për popullatën e Republikës së Maqedonisë.
7. Bashkëpunimi i palëve të interesuara në drejtim të zhvillimit dhe zbatimit të teknologjive që do të sigurojnë mbrojtje dhe transparencë maksimale, si dhe testim dhe vlerësim të nivelit të sigurisë së teknologjive të përdorura.
8. Bashkëpunimi me palët e interesuara në projekte kërkimore në nivel kombëtar dhe ndërkombëtar.
9. Organizimi dhe pjesëmarrja në aktivitete dhe iniciativa të ndryshme ndërkombëtare në fushën e sigurisë kibernetike.
10. Krijimi i mekanizmave dhe procedurave për bashkëpunim ndërkombëtar në nivel diplomatik në rast të incidenteve, sulmeve dhe krizave kibernetike, në përputhje me parimet e vendosura në nivel ndërkombëtar.

11. Promovimi dhe avancimi i normave, rregullave dhe parimeve të sjelljes së përgjegjshme nga shteti, në përputhje me parimet e vendosura në nivel ndërkombëtar.
12. Krijimi dhe promovimi i bashkëpunimit dhe krijimi i besimit me ekipet e tjera ndërkombëtare publike dhe private të CERT dhe CSIRT, komunitetet akademike dhe organizata të tjera ndërkombëtare.
13. Bashkëpunimi i të gjitha palëve të interesuara për krijimin e legjislacionit kombëtar, si dhe kontribut në përcaktimin e legjislacionit ndërkombëtar lidhur me mënyrën e sjelljes në hapësirën kibernetike, lirinë e shprehjes, mbrojtjen e të dhënave personale, të drejtat e privatësisë dhe të drejtat dhe liritë themelore të njeriut.
14. Bashkëpunimi i të gjitha palëve të interesuara për unifikimin e normave të sigurisë, standardizimin e bashkëpunimit dhe përcaktimin dhe vendosjen e një niveli të detyrueshëm të mbrojtjes për subjektet që menaxhojnë IKI dhe VIS.
15. Bashkëpunimi me sektorin privat për të ofruar një hapësirë kibernetike që ofron një mjedis të sigurt për shkëmbimin e informacionit, kërkimin dhe zhvillimin dhe ofrimin e një infrastrukture të sigurt informacioni që do të stimulojë sipërmarrjen në mënyrë që të mbështesë konkurrencën e të gjitha kompanive vendase dhe të mbrojë investimet e tyre.
16. Ndërtimi i besimit midis të gjithë aktorëve, duke përfshirë krijimin e një platforme/sistemi kombëtar për shkëmbimin e informacionit në lidhje me kërcënimet, incidentet dhe rreziqet e menjëhershme.

Zbatimi

Pas miratimit të Strategjisë Kombëtare për Sigurinë Kibernetike, brenda tre muajve hartohet një Plan Veprimi për zbatimin e qëllimeve dhe aktiviteteve të përcaktuara në Strategji. Autoritetet përgjegjëse për zbatimin e qëllimeve dhe aktiviteteve të parapara përcaktohen sipas kësaj Strategjie. Zbatimi i masave të strategjisë do të

koordinohet nga Këshilli Kombëtar i Sigurisë Kibernetike. Në përputhje me strategjinë, ministritë dhe institucionet kompetente do të bëjnë një analizë të legjislacionit dhe, nëse është e nevojshme, do të harmonizojnë rregulloret dhe procedurat në departamentin e tyre. Ministritë kompetente do të dorëzojnë raporte periodike të zbatimit në Këshillin Kombëtar të Sigurisë Kibernetike. Në varësi të nevojës së treguar, Strategjia e Sigurisë Kibernetike mund të rishikohet dhe përditësohet.

Për këtë qëllim, Republika e Maqedonisë do të themelojë**Këshilli Kombëtar i Kibernetikës**sigurinë dhe**Një organ me aftësi operacionale për sigurinë kibernetike**.

Këshilli Kombëtar i Sigurisë Kibernetike

Me qëllim të koordinimit dhe monitorimit të aktiviteteve të kryera në përputhje me Strategjinë për siguri kibernetike, Planin e veprimit, si dhe përcaktimin e drejtimeve dhe rekomandimeve të reja strategjike lidhur me segmentin e sigurisë kibernetike, Qeveria e Republikës së Maqedonisë do të të krijojë një Këshill Kombëtar për Sigurinë Kibernetike i cili do të ketë aktivitete në drejtim të:

- Monitorimi dhe koordinimi sistematik i zbatimit të Strategjisë Kombëtare të Sigurisë Kibernetike dhe shqyrtimi i të gjitha sfidave në fushën e sigurisë kibernetike.
- Propozimi i masave specifike për përmirësimin e zbatimit të Strategjisë dhe Planit të Veprimit për zbatimin e Strategjisë së Sigurisë Kibernetike.

- Ai propozon shtesa dhe ndryshime në Strategjinë dhe Planin e Veprimit për të përballuar në mënyrë më efektive sfidat e reja në fushën e sigurisë kibernetike.
- Identifikimi i sfidave për menaxhimin e krizave kibernetike dhe propozimi i masave të duhura për efikasitet më të madh.
- Pjesëmarrja, koordinimi dhe respektimi i aktiviteteve të Këshillit të Sigurimit të Republikës së Maqedonisë.

- Analiza e situatës aktuale të sigurisë bazuar në raportet e marra nga organi me aftësi operacionale për sigurinë kibernetike.
- Miratimi i planit të masave dhe aktiviteteve për reagim në rast krize kibernetike, të propozuar nga organi me kapacitete operacionale për sigurinë kibernetike.
- Zhvillimi i programeve dhe planeve të veprimit për aktivitetet në fushën e sigurisë kibernetike që do të ndërmerr organi me kapacitete operacionale për sigurinë kibernetike.

Një organ me aftësi operacionale për sigurinë kibernetike

Organi me kapacitete operacionale për sigurinë kibernetike mund të formohet si organ i pavarur (agjenci, drejtori) i sapoformuar ose si njësi organizative e sapoformuar, pra organ në kuadër të një organi ekzistues.

Organi me kapacitete operacionale do të kishte kompetencën për të funksionalizuar aktivitetet e identifikuara që përcaktohen në Strategjinë e Sigurisë Kibernetike dhe Planin e Veprimit dhe udhëzimet dhe rekomandimet e dhëna nga Këshilli Kombëtar i Sigurisë Kibernetike, me kompetenca bazë:

- Zhvillimi dhe ofrimi i rekomandimeve, opinioneve, raporteve, hulumtimeve dhe udhëzimeve në lidhje me zbatimin e Strategjisë së Sigurisë Kibernetike, Planit të Veprimit dhe dokumenteve të tjera strategjike që lidhen me sigurinë kibernetike.

- Monitorimi i tendencave në sigurinë e hapësirës kibernetike për të zbuluar kërcënimet që mund të rezultojnë në një krizë kibernetike.
- Krijimi dhe shkëmbimi i vlerësimeve periodike të gjendjes së sigurisë kibernetike.

- Bashkëpunim i vazhdueshëm dhe shkëmbim informacioni mbi kërcënimet kibernetike, dobësitë, incidentet, rreziqet dhe statistikat e funksionimit me të gjitha palët e interesuara.
- Propozimi i një plani masash dhe aktivitetesh për reagim në rast të një krize kibernetike.
- Propozimi, zbatimi dhe pjesëmarrja në ushtrime kombëtare dhe ndërkombëtare në fushën e sigurisë kibernetike.
- Zhvillimi i kapaciteteve për asistencë operative për subjektet në përballjen e sulmeve në shkallë të gjerë.
- Regjistrimi i gjendjes aktuale të TIK-ut të çdo të interesuari (përdoruesi i shërbimeve të këtij organi) dhe paraqitja e raporteve të rregullta për ndryshimet apo incidentet e regjistruara nga të gjitha subjektet për të dhënë një alarm parandalues për abuzime të mundshme të atyre sistemeve.
- Monitorimi i zbatimit të aktiviteteve të parashikuara nga Strategjia e Sigurisë Kibernetike dhe dokumentet e tjera strategjike dhe standardet ndërkombëtare, nga të gjitha palët e interesuara (përdoruesit) e shërbimeve të organit me aftësi operacionale për sigurinë kibernetike.
- Aktivitetet e koordinimit dhe konsultimit gjatë zbatimit të zgjidhjeve të reja të TIK-ut dhe zhvillimit të zgjidhjeve softuerike për të gjithë palët e interesuara (përdoruesit) e shërbimeve të këtij organi.

Sfidat e zbatimit

Sfidat më të mëdha në zbatimin e Strategjisë së Sigurisë Kibernetike mund të jenë niveli i ulët i ndërgjegjësimit për rëndësinë e një hapësire të sigurt kibernetike, mungesa e higjienës kibernetike, si dhe mungesa e vullnetit politik dhe konsensusit për një qasje sistematike në tejkalimin e sfidave që lidhen me sigurinë kibernetike. Një qasje josistematike mund të shkaktojë pasoja të dëmshme për shtetin, veçanërisht kur shoqëria përballet me sulme të avancuara kibernetike në një shkallë më të gjerë.

Krijimi i bashkëpunimit efektiv ndërmjet palëve të interesuara është gjithashtu një nga sfidat më të mëdha gjatë zbatimit të strategjisë. Bashkëpunimi në fushën e sigurisë kibernetike është në shumë raste i ri për disa aktorë publikë dhe kërkon ndryshim zakonesh. Sfida kryesore në fushën e bashkëpunimit janë interesat dhe kompetencat e ndryshme të aktorëve të ndryshëm.

Përveç sa më sipër, besimi ndërmjet sektorit publik dhe atij privat mund të jetë një nga pengesat kryesore në zbatimin efektiv të Strategjisë së Sigurisë Kibernetike. Krijimi i besimit është një proces që kërkon dialog, si dhe kohë dhe përpjekje shtesë. Për shkak të mosbesimit, disa institucione dhe organizata nuk janë të gatshme të raportojnë incidente të sigurisë, kryesisht për shkak të humbjes së mundshme të reputacionit. Mungesa e shkëmbimit të informacionit dhe mungesa e detyrimit për raportimin e incidenteve çon në ndërgjegjësimin e pamjaftueshëm të situatës aktuale me kërcënimet kibernetike, gjë që mund të jetë shkaku i vështirësive në zbatimin e aktiviteteve për t'iu kundërvënë sfidave tashmë të njohura në hapësirën kibernetike.

Sfidë e madhe në zbatimin e Strategjisë për Siguri Kibernetike të Republikës së Maqedonisë mund të jetë mungesa e burimeve financiare dhe kuadrove të kualifikuara për t'u përballur me sfidat në hapësirën kibernetike.

Zbatimi i suksesshëm i Strategjisë së Sigurisë Kibernetike do të ketë një ndikim pozitiv në rritjen e sigurisë kibernetike dhe duke siguruar kështu

Siguria Kombetare. Përveç kësaj, ofrimi i hapësirës kibernetike do të rrisë besimin e përdoruesve në hapësirën kibernetike, që mund të ketë një kontribut të rëndësishëm në zhvillimin e shërbimeve të reja të bazuara në internet dhe kjo do të shkaktojë rritje ekonomike në Republikën e Maqedonisë.

ANEKSI 1

Përkufizimet

Botnet- një rrjet kompjuterash privatë të infektuar me softuer me qëllim të keq dhe të kontrolluar kolektivisht pa dijeninë e pronarëve

Organizatat civile- çdo shoqatë, fondacion, sindikatë, si dhe çdo formë organizative e një organizate të huaj, si dhe çdo formë tjetër e shoqatës, e regjistruar në përputhje me dispozitat e Ligjit për shoqatat dhe fondacionet, por edhe lëvizjet civile joformale ose grupet e qytetarët që merren me iniciativa nga fusha e mbrojtjes së të drejtave dhe lirive të njeriut.

Backdoor– një teknikë në të cilën mekanizmi i sigurisë së një sistemi anashkalohet në mënyrë të padukshme për të siguruar akses në një sistem informacioni ose në të dhënat e tij.

Malware- softuer që është krijuar posaçërisht për të prishur, dëmtuar ose për të fituar akses të autorizuar në një sistem informacioni.

Sistemet e kontrollit industrial- Sistemet e informacionit në SCADA (kontrolli mbikëqyrës dhe grumbullimi i të dhënave) dhe grupet e sistemeve të kontrollit të shpërndarë, të përdorura për operacione industriale, si prodhimi, kontrolli i prodhimit dhe kontrolli i shpërndarjes nëpërmjet kontrolluesve logjikë të programueshëm që janë të ndryshëm nga teknologjitë konvencionale të informacionit.

Internet- një rrjet global kompjuterik që siguron lidhjen e pajisjeve të informacionit dhe komunikimit dhe sistemeve të lidhura me to duke përdorur protokolle të standardizuara të komunikimit.

Siguria e informacionit- gjendja e konfidencialitetit, integritetit dhe disponueshmërisë së informacionit, e arritur me zbatimin e masave të duhura të sigurisë.

Sistemet e informacionit- Sistemet e përfshira në ofrimin e çdo shërbimi, transaksioni dhe informacioni/të dhënash nëpërmjet TIK-ut.

Informacion i klasifikuar- informacion që mbrohet nga aksesi ose përdorimi i paautorizuar dhe që përcaktohet nga niveli i klasifikimit.

Infrastruktura e informacionit kritik(KII) - çdo sistem informacioni-komunikimi, mirëmbajtja, siguria dhe siguria e të cilit janë kritike për sigurinë kombëtare, ekonominë, sigurinë publike dhe shëndetin. Infrastruktura kombëtare e informacionit kritik është pjesë e infrastrukturës kritike (CI).

Kriptovalutat– monedha virtuale të decentralizuara, të bazuara në parime matematikore dhe të mbrojtura nga algoritme kriptografike, ku parimet e kriptografisë përdoren për të zbatuar një ekonomi informacioni të shpërndarë, të decentralizuar dhe të sigurt.

Të dhënat personale - çdo informacion që i referohet një personi fizik të identifikuar ose një personi fizik të identifikueshëm, dhe një person i identifikueshëm është një person, identiteti i të cilit mund të përcaktohet drejtpërdrejt ose tërthorazi, veçanërisht në bazë të numrit të identifikimit të një qytetari ose në bazë të një ose më shumë veçorive. specifik për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor ose social;

Autoritetet -organet e administratës shtetërore, organet e tjera shtetërore, organet në kuadër të ministrive, organizatat administrative dhe organet e pavarura, organet gjyqësore dhe gjykatat, organet e komunave, qytetit të Shkupit dhe komunave të qytetit të Shkupit, si dhe persona juridikë dhe të tjerë të cilëve me ligj atyre u është besuar ushtrimi i pushteteve publike. Në këtë kontekst, termi subjekte të tjera i referohet: personave juridikë që ofrojnë dhe ofrojnë shërbime me interes publik, pra subjekte nga fusha e arsimit, shëndetësisë, financës, bankave, sigurimeve, energjetikës, furnizimit me ujë, komunikimeve elektronike, shërbimeve postare. dhe shërbimet komunale.

Siguria kombetare -një sistem për një formë moderne të organizimit dhe funksionimit të shoqërisë me qëllim të zbatimit të aktiviteteve dhe masave specifike në një plan parandalues dhe represiv për të mbrojtur vlerat themelore shoqërore nga të gjitha llojet dhe format e sfidave, kërcënimeve dhe rreziqeve të sigurisë. nivelet.

Ransomware– një lloj softueri me qëllim të keq i krijuar për të bllokuar aksesin në një sistem informacioni ose në të dhënat e ruajtura në atë sistem, zakonisht nëpërmjet enkriptimit, ku një sasi e caktuar parash zhvatet nga viktima, e cila nga ana tjetër i ofrohet mundësia për të deshifruar sistemin e informacionit ose të dhëna.

ndërgjegjja- i referohet ndërgjegjësimit për sigurinë e të gjithë personave që ndajnë përgjegjësinë për sigurinë e informacionit.

Siguria kibernetike- aktivitetet dhe masat për të mbrojtur sistemet e informacionit që formojnë hapësirën kibernetike nga sulmet, duke siguruar konfidencialitetin, integritetin dhe disponueshmërinë e informacionit dhe sistemeve, zbulimin e sulmeve dhe incidenteve të sigurisë kibernetike, aktivizimin e mekanizmave kundërpërgjigje dhe rivendosjen e sistemeve në një gjendje në të cilën ishin para incidentit kibernetik.

Lufta kibernetike- një akt lufte brenda dhe rreth hapësirës virtuale me mjete që lidhen kryesisht me teknologjinë e informacionit.

Kërcënimi kibernetik- shkaku i mundshëm i një incidenti në hapësirën kibernetike që mund të shkaktojë dëme në një institucion ose sistem.

Incidenti kibernetik- një ose më shumë ngjarje që lidhen me sigurinë kibernetike që shkaktojnë shkelje të konfidencialitetit, integritetit ose disponueshmërisë së informacionit dhe cenojnë sigurinë e sistemit të informacionit.

Kriza kibernetike- ngjarje ose ngjarje në hapësirën kibernetike që mund të shkaktojnë ose tashmë kanë shkaktuar përçarje të konsiderueshme në jetën shoqërore, politike dhe ekonomike të Republikës së Maqedonisë. Një situatë e tillë mund të ndikojë në sigurinë e qytetarëve, në sistemin demokratik, në sistemin politik

stabilitetin, ekonominë, mjedisin dhe vlerat e tjera kombëtare, pra sigurinë kombëtare dhe mbrojtjen në përgjithësi.

Krimi kibernetik– mbulon aktivitetet e paligjshme që kryhen në hapësirën kibernetike, pra krimet që mund të kryhen vetëm nëpërmjet përdorimit të pajisjeve dhe sistemeve të TIK-ut, ku pajisjet dhe sistemet ose përdoren si mjete për kryerjen e

krimeve, ose janë objektivat kryesore të kriminalitetit. aktivitetet; ose krimi i mundësuar nga hapësira kibernetike, si aktivitetet tradicionale kriminale dhe materialet e abuzimit me fëmijët, i cili rritet me rritjen e përdorimit të kompjuterëve, rrjeteve kompjuterike ose formave të tjera të TIK-ut.

Hapësira kibernetike– një hapësirë në të cilën zhvillohet komunikimi ndërmjet sistemeve të informacionit. Në kuadër të Strategjisë, ky përkufizim mbulon internetin dhe të gjitha sistemet e informacionit të lidhura me të, si dhe sistemet e pavarura të informacionit.

Sulmi kibernetik- operacionet që personat dhe/ose sistemet e informacionit kryejnë qëllimisht në çdo vend në hapësirën kibernetike me qëllim që të kërcënojnë konfidencialitetin, integritetin ose disponueshmërinë e sistemeve të informacionit në hapësirën kombëtare kibernetike.

Mbrojtja kibernetike- një masë proaktive për të zbuluar ose marrë informacion në lidhje me një ndërhyrje kibernetike, sulm kibernetik ose operacion kibernetik ose për të përcaktuar origjinën e operacionit që përfshin përfshirjen e një operacioni parandalues ose kundër operacionit kibernetik kundër burimit.

Rezistenca kibernetike- aftësia për t'u përgatitur, përshtatur, përballuar dhe rikuperuar shpejt nga ndërprerjet që vijnë nga sulmet e qëllimshme, aksidentet ose kërcënimet natyrore ose incidentet në hapësirën kibernetike.

Rreziku kibernetik- rreziku i mundshëm për të shkaktuar dëme duke përdorur dobësitë në një ose më shumë entitete informacioni.

Sabotimi kibernetik– një sulm kibernetik i drejtuar kundër integritetit dhe disponueshmërisë së sistemeve të TIK.

Higjiena kibernetike- një referencë për praktikat dhe hapat që përdoruesit e pajisjeve dhe sistemeve të informacionit duhet të ndërmarrin për të ruajtur shëndetin e sistemit dhe për të përmirësuar sigurinë e internetit.

Spiunazhi kibernetik– një sulm kibernetik i drejtuar kundër besueshmërisë së sistemeve të TIK.

CERT- i referohet një ekipi emergjence që do të parandalojë kërcënimet dhe do të rivendosë sistemet e TIK nëse ndodhin incidente sigurie. Në thelb, CERT/CSIRT/CIRT ofron shërbime të reagimit ndaj emergjencave, shërbime parandaluese dhe menaxhim të cilësisë së sigurisë. Rrjeti CERT është të njëjtët njerëz që punojnë në sigurinë kibernetike. Forcimi i një shërbimi të sigurisë kibernetike dhe incidenteve kibernetike.

ANEKSI 2

Akronimet

TIK– Teknologjitë e informacionit dhe komunikimit**PËRFUNDOI**– Indeksi i Zhvillimit të E-Government
GCI– Indeksi Global i Sigurisë Kibernetike**ISHTE**- Indeksi i zhvillimit të TIK-ut
USHQIMI– Indeksi i gatishmërisë së rrjetit

OBSH- Infrastruktura e informacionit kritik**VIS**– Sisteme të rëndësishme informacioni
Të– Refuzimi i shërbimit

DDoS– Refuzim i shpërndarë i shërbimit

CERT– Ekipi i Reagimit të Emergjencave Kompjuterike**E DREJTË**– Ekipi i reagimit ndaj incidenteve kompjuterike

KEMËR– Ekipi i reagimit ndaj incidenteve të sigurisë kompjuterike**SCADA**– kontrolli mbikëqyrës dhe mbledhja e të dhënave

E U- Bashkimi Europian

NATO– Organizimi i Traktatit të Atlantikut të Veriut

MKD-CIRT-Qendra Kombëtare e Reagimit ndaj Incidenteve Kompjuterike

Pjesëmarrësit në përgatitjen e dokumentit:

Dimitar Mançev - Ministria e Shoqërisë Informatike dhe të Administratës, Solza Kovaçevska - Ministria e Shoqërisë Informative dhe të Administratës, Ana Maltseva - Ministria e Shoqërisë Informatike dhe të Administratës - Marjan Stoilkovski, Ministria e Punëve të Brendshme

Natalija Veljanoska - Ministria e Punëve të Brendshme, Jane Stojanov - Ministria e Punëve të Brendshme, Alenka Gjordjieva - Ministria e Mbrojtjes

Mitko Bogdanoski - Ministria e Mbrojtjes, Filip Stojkovski - Ministria e Mbrojtjes, Orhan Ismaili - Ministria e Mbrojtjes

Jovana Gjorgjioska - Ministria e Shoqërisë Informatike dhe e Administratës, Elena Mançeva - Ministria e Shoqërisë Informative dhe e Administratës