Politika për Rritjen e Kapaciteteve të Institucioneve për Sigurinë Kibernetike

PËRMBAJTJA

1. Hyrje

Politika për Rritjen e Kapaciteteve të Institucioneve për Sigurinë Kibernetike është një hap i rëndësishëm drejt rritjes së sigurisë kibernetike në Shqipëri. Kjo politikë synon rritjen e kapaciteteve institucionale për parandalimin, adresimin dhe reagimin efektiv ndaj rreziqeve dhe incidenteve kibernetike, si dhe mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit, duke kontribuar në forcimin e sigurisë kombëtare.

2. Përshkrimi i Politikës

Politika për Rritjen e Kapaciteteve të Institucioneve për Sigurinë Kibernetike ka për qëllim adresimin e sfidave sa i përket kapaciteteve teknike dhe njerëzore të institucioneve publike dhe private në nivel kombëtar duke parashikuar masat që duhet të ndërmerren për rritjen e kapaciteteve me qëllim forcimin e sigurisë kibernetike.

Me rritjen e zhvillimit të teknologjisë dhe digjitalizimin e shërbimeve në Shqipëri, janë shtuar edhe rreziqet në hapësirën kibernetike. Kohët e fundit është vënë re një tendencë në rritje e incidenteve kibernetike që shenjëstrojnë infrastrukturat kritike dhe të rëndësishme të informacionit, si publike ashtu edhe private. Me shtimin e rreziqeve dhe incidenteve kibernetike, përgjigja efektive ndaj tyre është e domosdoshme, por për këtë, nevojiten kapacitete teknike dhe njerëzore institucionale. Mungesa e kapaciteteve dhe burimeve të nevojshme, përbën një sfidë që duhet adresuar. Pasojat që incidentet mund të kenë në infrastrukturat e informacionit mund të cenojnë rëndë sigurinë kombëtare dhe ekonominë, rrjedhimisht nevojitet që të ndërmerren veprime për rritje kapacitetesh të institucioneve në nivel kombëtar për të garantuar sigurinë dhe mbrojtjen nga sulmet e ndryshme të aktorëve keqdashës në hapësirën kibernetike.

Në këtë kontekst, Politika për Rritjen e Kapaciteteve të Institucioneve për Sigurinë Kibernetike do të adresojë mungesën e kapaciteteve duke përcaktuar masat konkrete për rritjen e kapaciteteve njerëzore, kapaciteteve teknike, si dhe masat për krijimin e mekanizmave të nevojshëm dhe rritjen e bashkëpunimit kombëtar dhe ndërkombëtar, në funksion të ngritjes dhe forcimit të kapaciteteve.

3. Misioni dhe Qëllimet

Misioni i politikës është rritja e kapaciteteve dhe efikasitetit të institucioneve përgjegjëse për sigurinë kibernetike në Shqipëri për të parandaluar dhe për t'u kundërpërgjigjur ndaj kërcënimeve kibernetike, me qëllim ruajtjen e stabilitetit dhe sigurisë kombëtare.

Qëllimet e politikës janë:

- Forcimi i kapaciteteve ekzistuese dhe ngritja e kapaciteteve të reja institucionale në fushën e sigurisë kibernetike
- Rritja e kapaciteteve, masave dhe mjeteve teknike, për t'u mbrojtur dhe përgjigjur ndaj sulmeve kibernetike
- Rritja dhe përmirësimi i kapaciteteve njerëzore të specializuara në siguri kibernetike
- Krijimi dhe forcimi i mekanizmave të bashkëpunimit kombëtar dhe ndërkombëtar me synim rritjen e kapaciteteve në fushën e sigurisë kibernetike

4. Fusha e Zbatimit

Kjo politikë zbatohet nga të gjitha institucionet publike, agjencitë shtetërore dhe strukturat që ofrojnë shërbime publike digjitale ose menaxhojnë sisteme dhe të dhëna me rëndësi për funksionimin e shtetit. Kjo politikë synon te adresoj një qasje gjithëpërfshirëse për ndërtimin e kapaciteteve për institucionet publike dhe private.

Politika shërben si dokument udhëzues për hartimin e planeve të brendshme për rritjen e kapaciteteve dhe për integrimin e sigurisë kibernetike në politikat e menaxhimit të burimeve njerëzore, të teknologjisë dhe të organizimit institucional.

5. Parimet Themelore

Zbatimi i kësaj politike mbështetet në parimin se kapacitetet institucionale duhet të ndërtohen në mënyrë të qëndrueshme dhe afatgjatë . Politika thekson rëndësinë e zhvillimit të vazhdueshëm profesional të stafit dhe të përshtatjes së vazhdueshme të institucioneve me zhvillimet teknologjike.

Një tjetër parim thelbësor është integrimi i sigurisë kibernetike në strukturat ekzistuese të qeverisjes institucionale, në mënyrë që të mos trajtohet si funksion dytësor, por si pjesë e pandashme e menaxhimit dhe vendimmarrjes.

6. Mjete dhe Masa Konkrete

Kjo politikë është në përputhje me vizionin dhe objektivat e Strategjisë Kombëtare për Sigurinë Kibernetike 2025-2030 dhe përforcon masat për rritjen e kapaciteteve institucionale, publike dhe private.

Masat dhe veprimet konkrete do të detajohen në Planin e Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike, sipas nevojave dhe prioriteteve.Masat që do të merren për zbatimin e kësaj politike përfshijnë:

- Masa për rritjen e kapaciteteve të burimeve njerëzore
- Masa për rritjen e kapaciteteve teknike
- Masa për krijimin e mekanizmave të nevojshëm dhe rritjen e bashkëpunimit kombëtar dhe ndërkombëtar, në funksion të ngritjes dhe forcimit të kapaciteteve

<u>Masa për rritjen e kapaciteteve të burimeve njerëzore përfshijnë:</u>

- Krijimi i një sistemi të qëndrueshëm edukimi për të rinjtë që kërkojnë të specializohen në fushën e sigurisë kibernetike, përmes ngritjes dhe fuqizimit të Akademisë Kombëtare të Sigurisë Kibernetike, dhe rritjes së kapaciteteve dhe cilësisë së institucioneve arsimore në fushën e sigurisë kibernetike në vend.
- Hartimi i programeve të studimit dhe trajnimit në fushën e sigurisë kibernetike me qëllim krijimin e gjeneratës së re të ekspertëve të sigurisë kibernetike dhe përditësimi i kurrikulave ekzistuese të arsimit të lartë në fushën e sigurisë kibernetike në vazhdimësi.
- Organizimi dhe zbatimi i programeve kombëtare të trajnimit dhe realizimi i ushtrimeve kibernetike të përbashkëta, mbi parandalimin, menaxhimin, reagimin dhe hetimin e incidenteve kibernetike me stafin përgjegjës për sigurinë kibernetike të institucioneve publike dhe private në vend duke përfshirë të gjithë sektorët.

- Organizimi i trajnimeve dhe ushtrimeve (Table Top Exercise) për strukturat vendimmarrëse të nivelit të lartë, lidhur me komunikimin dhe menaxhimin e krizës kibernetike.
- Trajnime për rritjen e kapaciteteve në fushën e sigurisë kibernetike dhe diplomacisë kibernetike të stafeve të institucioneve përgjegjëse.

Masat për rritjen e kapaciteteve teknike përfshijnë:

- Rritja e buxhetit për CSIRT[1]-in kombëtar dhe CSIRT-et sektoriale për të siguruar mjetet teknike dhe infrastrukturat e nevojshme të sigurisë për monitorimin, mbrojtjen, menaxhimin, dhe reagimin ndaj incidenteve kibernetike.
- Ngritja e kapaciteteve teknike të Qendrës Kombëtare Operacionale të Sigurisë (SOC Kombëtar) për monitorimin pro aktiv dhe reaktiv, si dhe trajtimin e incidenteve kibernetike.
- Optimizmi i infrastrukturave të sigurisë dhe zgjerimi i kapaciteteve të mbulimit të sektorit qeveritar.
- Pajisja e institucioneve me mjetet dhe infrastrukturat e nevojshme hardware dhe software në përputhje me standardet e fundit, për detektimin dhe parandalimin të sulmeve kibernetike potenciale.
- Zhvillimi i kapaciteteve teknike monitoruese, vlerësuese, analizuese dhe reaguese të CSIRT-eve dhe Drejtorisë për Hetimin e Krimeve Kibernetike pranë Policisë së Shtetit.
- Ngritja e laboratorëve të analizës së programeve keqdashëse, hetimit kibernetik dhe simulimit të incidenteve kibernetike.
- Krijimi i një platforme të re të dedikuar për raportimin e përmbajtjeve të paligjshme online që targetojnë femijët dhe të rinjtë, në bashkëpunim me Policinë e Shtetit.
- Implementimi i teknikave dhe procedurave të avancuara dhe të përmirësuara, për sigurinë dhe mbrojtjen kibernetike
- Kryerja e analizave të vazhdueshme të riskut dhe konformitetit, si dhe të kapaciteteve teknike, me qëllim identifikimin dhe adresimin e nevojave në vazhdimësi.

Masat për krijimin e mekanizmave të nevojshëm dhe rritjen e bashkëpunimit kombëtar dhe ndërkombëtar, në funksion të ngritjes dhe forcimit të kapaciteteve

- Hartimi dhe nënshkrimi i marrëveshjeve të bashkëpunimit me shtete, agjenci, si dhe qendra rajonale apo ndërkombëtare në fushën e sigurisë kibernetike me qëllim rritjen e kapaciteteve.
- Hartimi dhe nënshkrimi i marrëveshjeve të bashkëpunimit me universitetet sa i përket përditësimit të kurrikulave dhe zhvillimit të kërkimit shkencor në fushën e sigurisë kibernetike.
- Bashkëpunimi me Ministrinë e Arsimit dhe Sportit për mundësimin e një sistemi të qëndrueshëm edukimi në fushën e sigurisë kibernetike (krijimin dhe akreditimin e Akademisë Kombëtare të Sigurisë Kibernetike, përmirësimin e kurrikulave, dhe rritjen e cilësisë së arsimit të lartë lidhur me programet e studimit të sigurisë kibernetike).

[1] Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike - Computer Security Incident Response Team (CSIRT)

- Thellimi i bashkëpunimit me organizatat ndërkombëtare për shkëmbimin e ekspertizës teknike dhe informacionit në lidhje me kërcënimet kibernetike dhe dobësitë, si dhe për reagimin ndaj incidenteve të sigurisë kibernetike.
- Lidhja e marrëveshjeve të bashkëpunimit në fushën e sigurisë dhe krimit kibernetik midis institucioneve përkatëse në nivel kombëtar, me qëllim rritjen e kapaciteteve dhe shkëmbimin e njohurive dhe informacionit.
- Implementimi i projekteve dhe iniciativave të përbashkëta me partnerë ndërkombëtarë me qëllim rritjen e kapaciteteve në fushën e sigurisë kibernetike.

7.Bashkëpunimi dhe Partnerët

Partnerët në nivel kombëtar për zbatimin e kësaj politike përfshijnë subjektet e sektorit publik dhe privat, organizatat e shoqërisë civile, si dhe ekspertët për të ndarë njohuritë dhe përvojën. Ndërsa sa i përket bashkëpunimit ndërkombëtar, partnerë do të jenë organizatat ndërkombëtare ku Shqipëria është vend anëtar ose vend kandidat, si dhe agjencitë ndërkombëtare të qeverive të vendeve të tjera aleate dhe partnere strategjike, për të përforcuar kapacitetet mbrojtjetëse dhe përgjigjen ndaj kërcënimeve kibernetike dhe rritur sigurinë kibernetike në nivel kombëtar.

8.Monitorimi dhe Vlerësimi

Monitorimi i politikës do të zhvillohet duke analizuar implementimin e veprimeve të parashikuara në këtë politikë si dhe veprimeve të parashikuara në Planin e Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike që janë në linjë me objektivat e kësaj politike, përmes takimeve me institucionet përgjegjëse për zbatim dhe raporteve të monitorimit. Monitorimi kryhet në bazë raportesh 6-mujore ose vjetore dhe raportimeve nga institucionet përgjegjëse për zbatimin e masave. Në përfundim, hartohet raporti i monitorimit dhe nxirren përfundimet përkatëse, mbi bazën e të cilave propozohet përmirësimi i masave, kur vlerësohet i nevojshëm.

9.Financimi dhe kalendari i zbatimit

Zbatimi i aktiviteteve të parashikuara për implementimin e kësaj politike do të financohen nga buxheti i shtetit dhe donatorë të ndryshëm. Një financim i mirë-planifikuar do të mundësojë arritjen e rezultateve në përputhje me objektivat e kësaj politike dhe objektivat e Strategjisë Kombëtare për Sigurinë Kibernetike.

Kjo politikë do të zbatohet në përputhje me afatet e planifikuara në kalendarët e zbatimit për secilën nga masat e parashikuara. Kalendari i zbatimit hartohet çdo vit dhe si rrjedhojë shtrihet në një afat kohor një vjeçar.

10.Referencat

Kjo politikë mbështetet në legjislacionin kombëtar për sigurinë kibernetike, Strategjinë Kombëtare për Sigurinë Kibernetike, si dhe në praktikat dhe standardet ndërkombëtare të njohura në fushën e zhvillimit të kapaciteteve për sigurinë kibernetike.

11.Frekuenca e Rishikimit

Ky dokument duhet të rishikohet të paktën një herë në vit ose kur ka ndryshime të rëndësishme në sistemin e menaxhimit të sigurisë së informacionit në institucion.