# Ndërtimi i një ekosistemi digjital të sigurt dhe të qëndrueshëm:

# Adresimi i sfidave kryesore të sigurisë kibernetike në Kosovë

**Lëvizja FOL**
**2023**

# Ndërtimi i një ekosistemi digjital të sigurt dhe të qëndrueshëm:

# Adresimi i sfidave kryesore të sigurisë kibernetike në Kosovë

Lëvizja FOL

Në mbarë botën, njerëzit dhe shoqëritë kanë përfituar shumë nga revolucioni digjital, por ai gjithashtu ka sjellë rreziqe dhe sfida të reja. Kërcënimet kibernetike duke përfshirë sulmet kibernetike, shkeljet e të dhënave dhe mashtrimet në internet janë më të shpeshta dhe më të sofistikuara se kurrë më parë, duke paraqitur rreziqe serioze për njerëzit, kompanitë dhe infrastrukturën jetike. Ashtu si shumë vende të tjera, Kosova duhet të ndërmarrë hapa proaktivë për t'i zgjidhur këto çështje pasi përballet me to.

Me një popullsi prej rreth 1.8 milionë banorësh, Kosova është një vend i vogël, në rajonin e Ballkanit të Evropës. Me adoptimin e teknologjive të reja dhe rëndësinë në rritje të ekonomisë digjitale, Kosova po kalon një transformim digjital. Megjithatë, ky ndryshim sjell edhe sfida të reja të sigurisë kibernetike, pasi kërcënimet kibernetike vazhdojnë të rriten dhe evoluojnë.

Kjo përmbledhje e politikave fokusohet në çështjet kryesore të sigurisë kibernetike me të cilat po përballet Kosova tani dhe në zgjidhjet që mund të zbatohen. Përmes kësaj përmbledhje, do të identifikojmë tre çështje kyçe: kornizën joadekuate legjislative dhe rregullatore, kapacitetin e ulët të sigurisë kibernetike dhe mungesën e ndërgjegjësimit për sigurinë kibernetike. Po ashtu, do hulumtojmë se si sulmet kibernetike ndikojnë në infrastrukturën thelbësore të Kosovës, duke përfshirë bankën qendrore, qeverinë, ofruesin e telekomit dhe sistemin e shpërndarjes së energjisë elektrike.

Duke i zgjidhur këto çështje, Kosova mund të forcojë pozicionin e saj të sigurisë kibernetike dhe të krijojë një ekosistem digjital që është edhe i sigurt dhe i qëndrueshëm. Është e nevojshme një strategji me shumë palë të interesuara që të përfshijë sektorin publik, komunitetin e biznesit, shoqërinë civile dhe individët. FOL bën thirrje për një investim të vazhdueshëm në kornizat rregullatore, ndërtimin e kapaciteteve dhe iniciativat për rritjen e ndërgjegjësimit në sigurinë kibernetike. Objektivi përfundimtar është garantimi i infrastrukturës jetike të epokës digjitale, ndërmarrjeve dhe banorëve të Kosovës.

*This policy brief is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of Lëvizja FOL and do not necessarily reflect the vieës of USAID or the United States Government.*

# 1. Kuadri ligjor dhe rregullator:

Mungesa e një kuadri të plotë ligjor dhe rregullator për sigurinë kibernetike në Kosovë paraqet një problematikë në vete. Ani pse krimi kibernetik aktualisht trajtohet në mënyrë specifike me ligj, sistemi aktual ligjor nuk është mjaft i gjerë për të trajtuar në mënyrë adekuate rreziqet kibernetike. Mjedisi jashtëzakonisht i dobët legjislativ dhe rregullator i Kosovës për sigurinë kibernetike krijon pengesa serioze për luftimin e krimit kibernetik dhe ruajtjen e informacionit personal. Detajet e mëposhtme theksojnë këtë problem:

⇒ ***Mungesa e ligjeve specifike për krimin kibernetik*:** Kosova ka vënë në fuqi një ligj specifik për krimin kibernetik, në fund të shkurtit 2023. Edhe pse ekzistojnë dispozita në kodin penal të vendit që kanë të bëjnë me krimet e lidhura me kompjuterin, si qasja e paautorizuar në sistemet kompjuterike, jo të gjitha llojet e krimit kibernetik mbulohen nga këto dispozita.[1] Me miratimin e Ligjit për Sigurinë Kibernetike, janë shfuqizuar disa dispozita të dy ligjeve të cilat kanë qenë në fuqi prej vitit 2010 dhe 2012: Ligjit per Parandalimin dhe Luftimin e krimit kibernetik dhe Ligjit per Komunikimet Elektronike.

⇒ ***Legjislacioni për Mbrojtjen e të Dhënave Personale:*** Kosova e miratoi Ligjin për Mbrojtjen e të Dhënave Personale në vitin 2019. Edhe pse Kosova nuk është shtet anëtar i BE-së, ligji shprehimisht përputhet me GDPR-në dhe, ngjashëm me GDPR-në, përcakton të drejtat e subjektit të të dhënave, siç është e drejta të aksesit, të drejtës për korrigjim dhe të drejtës për fshirje. Ndërsa ligji nuk kërkon që organizatat të regjistrohen në AIP përpara përpunimit të të dhënave personale, AIP-i ka mandat të lëshojë certifikata për organizatat që përpunojnë të dhëna. AIP ka kompetencën të vendosë gjoba për shkelje të ligjit deri në 40,000 € ose 2-4% të qarkullimit vjetor të vitit paraardhës.

⇒ ***Mbikëqyrja e kufizuar rregullatore:*** Korniza rregullatore e Kosovës për sigurinë kibernetike[2] është e ndarë, me shumë organizata të ngarkuara me aspekte të ndryshme të sigurisë kibernetike. Përvec ASK, asnjë instancë tjetër në vend nuk është përgjegjëse për menaxhimin e sigurisë kibernetike ose koordinimin e përpjekjeve në industri të ndryshme.

Qeveria e Kosovës ka ndërmarrë veprime të ndryshme për të forcuar mjedisin legjislativ dhe rregullator për sigurinë kibernetike me qëllim të zgjidhjes së këtyre çështjeve. Një plan i ri i sigurisë kibernetike, për shembull, u krijua nga qeveria në vitin 2019 dhe përfshin hapa për të forcuar kuadrin legjislativ dhe rregullator të sigurisë kibernetike. Megjithatë, për të krijuar një strukturë të plotë ligjore dhe rregullatore, e cila është në përputhje me praktikat më të mira globale, ende duhet bërë një punë e konsiderueshme.

---

[1]Ligji për veprat penale të Republikës së Kosovës Nr. 04/L-082 (2013). Marrë nga http://ëëë.gjykataeap.com/repository/docs/criminal_code_of_kosovo.pdf

[2]Strategjia e Sigurisë Kibernetike e Republikës së Kosovës 2019-2022. Marrë nga https://kryeministri.rks-gov.net/ëp-content/uploads/2022/10/2-Strategjia-e-Sigurise-e-Kosoves-ENG.pdf

Korniza aktuale ligjore dhe rregullatore për sigurinë kibernetike në Kosovë është e pamjaftueshme, me mangësi në mbrojtjen e të dhënave personale dhe mungesë të mbikëqyrjes adekuate rregullatore. Kosova, edhe pse ka krijuar një strukturë më të plotë legjislative dhe rregullatore që trajton privatësinë, mbrojtjen e të dhënave dhe krimin kibernetik, duhet ta vëjë në funksion të plotë. Bazuar në praktikat më të mira globale, kjo kornizë duhet të përditësohet vazhdimisht për të pasqyruar kërcënime të reja dhe në zhvillim.

Në anën tjetër, Ligji për Mbrojtjen e të Dhënave Personale[3] i ka dhënë rëndësi të veçantë të drejtave të subjektit të të dhënave, duke forcuar rolin e tij si pronar i vetëm i të dhënave, pasi të dhënat personale janë personale dhe i përkasin vetëm subjektit të të dhënave (personit fizik).

Pra, brenda kësaj:

- ⇒ Ju keni të drejtë të informoheni sa herë që një kontrollues përpunon të dhënat tuaja, nëse ato të dhëna janë marrë nga ju apo edhe në ato raste kur nuk janë marrë nga ju.
- ⇒ Për të ushtruar të drejtën e informimit: Ju keni të drejtë të aksesoni të dhënat tuaja sa herë që kontrolluesi konfirmon se po përpunon të dhënat tuaja personale.
- ⇒ Për të ushtruar të drejtën e aksesit në të dhënat tuaja; ju keni të drejtë t'i kërkoni kontrolluesit të korrigjojë të dhënat tuaja personale nëse janë të pasakta ose të paplota.
- ⇒ Për të ushtruar të drejtën e korrigjimit. Ju keni të drejtë t'i kërkoni kontrolluesit të fshijë të dhënat tuaja personale, nëse zbatohet një nga kushtet e përcaktuara në ligj .
- ⇒ Ushtroni të drejtën e fshirjes ('e drejta për t'u harruar'); Ju keni të drejtë të kërkoni nga kontrolluesi kufizimin e përpunimit të të dhënave personale nëse zbatohet një nga kushtet e parashikuara në ligj .
- ⇒ Për të ushtruar të drejtën e parashkrimit. Kur ju kërkoni nga kontrolluesi të drejtën e korrigjimit, fshirjes ose kufizimit të të dhënave personale, ai është i detyruar t'ia komunikojë këtë çdo marrësi të cilit i janë zbuluar të dhënat personale. Ju keni të drejtë të merrni të dhënat tuaja personale që i keni dhënë kontrolluesit për ju, në një format të caktuar dhe keni të drejtë t'ia transmetoni këto të dhëna një kontrolluesi tjetër.
- ⇒ Për të ushtruar të drejtën e transferimit të të dhënave. Ju keni të drejtë të kundërshtoni përpunimin e të dhënave personale në lidhje me ju, për shkak të një situate të veçantë personale, nëse përpunimi zbatohet në nenin 5, paragrafi 1, nënparagrafi 1.5 dhe 1.6. të Ligjit. Ju gjithashtu keni të drejtë të kundërshtoni nëse përpunimi është bërë për qëllime legjitime marketingu.
- ⇒ Të ushtrojë të drejtën e kundërshtimit. Ju keni të drejtë të mos i nënshtroheni një vendimi të bazuar vetëm në përpunimin automatik, duke përfshirë profilizimin që prodhon efekte që lidhen me ju ose ju prek në mënyrë të ngjashme.

Të gjitha këto të drejta, si e drejta për informim, e drejta për të aksesuar të dhënat, e drejta për korrigjim, e drejta për kufizim, e drejta e fshirjes, e drejta e kufizimit, e drejta për transferim, e drejta për të kundërshtuar, mund të kufizohen, nëse një kufizim i tillë respekton thelbin e të drejtave dhe lirive themelore dhe është një masë e nevojshme dhe proporcionale për të garantuar situata të caktuara siç përcaktohet në nenin 22 të ligjit.

[3] Ligji për Mbrojtjen e të Dhënave Personale. Marrë nga https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616&langid=2

# Dënimet:

Sipas nenit 4(1.1) të Ligjit për Komunikimet Elektronike [4], agjencia rregullatore përgjegjëse për vënien në fuqi të kornizës ligjore të Ligjit për Komunikimet Elektronike njihet si Autoriteti Rregullativ i Komunikimeve Elektronike dhe Postare.

Sipas nenit 101(1) të Ligjit për Komunikimet Elektronike, nëse një biznesmen shkel ligjet që përcaktojnë kërkesat për përfshirje në aktivitete të komunikimeve elektronike ose kërkesat për përdorimin e burimeve të komunikimeve elektronike, duke përfshirë të drejtat e konsumatorit ose përdoruesit, ARKEP mund të vendosë një gjobë deri në në 86,000 € për to.

Nëse një sipërmarrës shkel në mënyrë të përsëritur ose seriozisht nenin 101(1) të Ligjit për Komunikimet Elektronike, ARKEP mund t'i gjobisë ata deri në 10% të të ardhurave të tyre vjetore bruto nga aktivitetet që lidhen me komunikimet elektronike. Nëse është e vështirë ose e pamundur të përcaktohet vëllimi i një aktiviteti të tillë, RAECP mund ta gjobisë sipërmarrësin deri në 150,000 € (neni 101(2) i Ligjit për Komunikimet Elektronike). Një dënim deri në 3,000 € duhet të shqiptohet kur të ardhurat bruto vjetore të një sipërmarrësi janë më pak se 85,000 € dhe duhet të shqiptohet një gjobë deri në 10,000 € në rastet e shkeljeve të përsëritura ose thelbësore (neni 101(3) i Komunikimeve Elektronike Ligji).

# 2. Cookies dhe teknologji të tjera

Neni 86 (3) i Ligjit për Komunikimet Elektronike përshkruan një procedurë të heqjes dorë nga cookie[5]. Në përputhje me Ligjin e Komunikimeve Elektronike, pajtimtarit ose përdoruesit në fjalë duhet t'i jepet informacion i qartë dhe i plotë, duke përfshirë informacionin në lidhje me qëllimet e përpunimit, dhe duhet t'i jepet mundësia për të refuzuar një përpunim të tillë nga kontrolluesi i të dhënave.Në mënyrë të ngjashme, neni 86 (3) i Ligjit të Komunikimeve Elektronike nuk ndalon asnjë ruajtje teknike ose akses që kërkohet rreptësisht për të ofruar një shërbim të shoqërisë së informacionit që është kërkuar shprehimisht nga pajtimtari ose përdoruesi, ose që përdoret për të kryer ose për të lehtësuar transmetimi i një komunikimi përmes një rrjeti komunikimi elektronik.

Ligji për Mbrojtjen e të Dhënave Personale përcakton se kontrolluesi duhet të marrë masat e duhura për të dhënë çdo informacion të përmendur në nenet 12 dhe 13 të ligjit për mbrojtjen e të dhënave dhe çdo komunikim sipas neneve 14 deri në 21 dhe 33 të ligjit për mbrojtjen e të dhënave në lidhje me përpunimin e të dhënave personale. në mënyrë të qartë dhe gjithëpërfshirëse, përveç kërkesës për informacion të qartë dhe gjithëpërfshirës për qëllimin e mbledhjes dhe përpunimit të të dhënave sipas nenit 86(3) të Ligjit për Komunikimet Elektronike. Sipas nenit 11 (1) të Ligjit për Mbrojtjen e të Dhënave, informacioni do të komunikohet me shkrim ose me një metodë tjetër, duke përfshirë mjetet elektronike kur është e nevojshme.

---

[4] Ligji për Komunikimet Elektronike. Marrë nga https://gzk.rks-gov.net/ActDetail.aspx?ActID=2851&langid=2

[5] Cookies janë pjesë të vogla teksti të dërguara nga paisja juaj në faqet e internetit që vizitoni. Ato e ndihmojnë atë faqe interneti të mbajë mend informacionin rreth vizitës suaj, gjë që mund ta bëjë më të lehtë vizitën e faqes përsëri dhe ta bëjë faqen më të dobishme për ju.

Subjekti i të dhënave ka të drejtë të kërkojë nga kontrolluesi konfirmim nëse të dhënat personale që i përkasin atij janë duke u përpunuar, dhe në këtë rast, akses në të dhënat personale si dhe informacionin e mëposhtëm (neni 14(1) i Mbrojtjes së të Dhënave:

- **Marrësit e synuar ose kategoritë e marrësve të cilëve u janë dhënë ose do t'u zbulohen të dhënat personale, si dhe marrësit në vendet e treta ose organizatat ndërkombëtare;**
- **Kur është e mundur, periudhën e parashikuar për të cilën do të ruhen të dhënat personale, ose, nëse nuk është e mundur, kriteret e përdorura për të përcaktuar atë periudhë;**
- **E drejta për të bërë ankesë pranë AIP-së;**
- **Ekzistenca e së drejtës për të kërkuar nga kontrolluesi korrigjimin, fshirjen ose kufizimin e përpunimit të të dhënave personale që i përkasin subjektit të të dhënave ose për të kundërshtuar një përpunim të tillë**

# 3. Mungesa e ndërgjegjësimit për sigurinë kibernetike:

Me avancimin e teknologjisë dhe me rritjen e përdorimit të internetit, kërcënimi i sulmeve kibernetike është intensifikuar dhe ka shkaktuar pasoja të rënda në nivel global. Për të adresuar këtë problematikë, është e rëndësishme të përmirësojmë ndërgjegjësimin dhe edukimin e publikut të gjerë në lidhje me sigurinë kibernetike në të gjithë nivelet.

Kjo përfshin por nuk kufizohet në: ngritjen e ndërgjegjësimit të publikut përmes edukimit dhe trajnimit, zhvillimin e politikave dhe ligjeve të forta për sigurinë kibernetike, si dhe forcimin e kapaciteteve teknike për të parandaluar, zbuluar dhe trajtuar sulmet kibernetike.

Edhe pse ka pak informacion në dispozicion për vetëdijen e qytetarëve të Kosovës për sigurinë kibernetike, disa shenja tregojnë për një nivel të ulët të njohurive. Për shembull:

⇒ ***Mungesa e edukimit për sigurinë kibernetike:*** Sipas studimit të Indeksit të Ekonomisë dhe Shoqërisë Digjitale (DESI) nga Komisioni Evropian [6], vetëm 36% e njerëzve në Kosovë zotërojnë aftësitë më themelore digjitale, duke përfshirë të kuptuarit e sigurisë kibernetike. Kjo tregon se shumë njerëz mund të mos jenë të vetëdijshëm për rreziqet e përfshira në aktivitetet e internetit.

[6]Komisioni Europian. (2021). Indeksi i Ekonomisë dhe Shoqërisë Digjitale (DESI) 2021: Raporti i vendit - Kosovë. Marrë nga https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

⇒ ***Përdorimi i ulët i mjeteve të sigurisë kibernetike:*** Sipas një ankete [7]të Agjencisë Kosovare për Shoqëri Informative (AIS), vetëm 5% e bizneseve të vogla dhe të mesme (NVM) në Kosovë përdorin mure zjarri, dhe vetëm 18% e NVM-ve atje përdorin softuer antivirus. Kjo tregon se shumë kompani mund të mos e kuptojnë rëndësinë e teknologjive të sigurisë kibernetike në parandalimin e sulmeve kibernetike .

⇒ ***Raportimi i kufizuar i krimit kibernetik:*** Sipas të njëjtit hulumtim të AIS, vetëm 6% e NVM-ve në Kosovë [8]kanë informuar autoritetet për një rast të krimit kibernetik. Kjo nënkupton që shumë kompani mund të mos e kuptojnë rëndësinë e raportimit të ngjarjeve të krimit kibernetik ose mund të mos kuptojnë se si ta bëjnë këtë.

Këto nënkuptojnë se Kosova duhet të jetë më e ndërgjegjshme për çështjet e sigurisë kibernetike. Siç sugjerohet në përmbledhjen e politikave, një fushatë gjithëpërfshirëse kombëtare ndërgjegjësimi për sigurinë kibernetike mund të ndihmojë në zgjidhjen e këtij problemi duke shpërndarë njohuri rreth llojeve të shumta të kërcënimeve kibernetike dhe se si t'i dalloni dhe shmangni ato. Qeveria e Kosovës duhet të krijojë një fushatë kombëtare ndërgjegjësuese për sigurinë kibernetike për të informuar popullatën, kompanitë dhe institucionet qeveritare për rëndësinë e sigurisë kibernetike për të adresuar këtë problem. Kjo fushatë duhet t'i edukojë njerëzit për llojet e ndryshme të kërcënimeve kibernetike dhe si t'i dallojnë dhe shmangin ato.

# 4. Infrastruktura kritike e cenueshme ndaj sulmeve kibernetike:

Rrjetet e energjisë, ujit dhe telekomunikacionit të Kosovës janë të gjitha në rrezik nga sulmet kibernetike. Ekonomia dhe siguria e vendit mund të vuajnë ndjeshëm si rezultat i këtyre sulmeve. Sulmet kibernetike janë një mundësi kundër infrastrukturës jetike të Kosovës, duke përfshirë industrinë e energjisë elektrike dhe telekomunikacionit. Detajet e mëposhtme theksojnë këtë problem:

⇒ ***Sulmi në sektorin e energjisë:*** Në janar 2019, një sulm kibernetik në Sistemin e Shpërndarjes së Energjisë Elektrike të Kosovës rezultoi në një ndërprerje të energjisë elektrike që preku pothuajse 200,000 konsumatorë [9]. Një sulm i Mohimit të Shërbimit të Shpërndar (DDoS) u nis kundër sistemit nga sulmuesit duke përdorur malëare "XOR.DDoS". Kjo u shkaktua nga ndërprerja e operacioneve të monitorimit dhe kontrollit të sistemit nga sulmi. Kjo tregoi se sa i ndjeshëm është sektori i energjisë elektrike i Kosovës ndaj kërcënimeve online.

[7]Agjencia Kosovare për Shoqëri Informative. (2019). Anketa e Sigurisë Kibernetike për NVM-të në Kosovë. Marrë nga http://ais.al/ëp-content/uploads/2019/04/Cyber-security-survey-for-SMEs-in-Kosovo.pdf

[8] po aty

[9]Sistemi i Shpërndarjes së Energjisë Elektrike të Kosovës pëson një sulm të madh kibernetik. Marrë nga https://ëëë.crn.com.au/neës/kosovo-electricity-distribution-system-suffers-major-cyber-attack-517394

⇒ ***Sulmi në sektorin e telekomunikacionit:*** Firma e telekomunikacionit IPKO pësoi një sulm kibernetik që preku shërbimet e saj në tetor 2020[10]. Për të mposhtur serverët e kompanisë dhe për të ndaluar shërbimet e saj, sulmuesit filluan një sulm DDoS. Shërbimet e zërit, internetit dhe TV u prekën të gjitha për disa orë nga sulmi. Incidenti, një nga sulmet kibernetike më të rënda në historinë e Kosovës, ekspozoi dobësinë e industrisë së telekomunikacionit të vendit.

⇒ ***Sulmi në sektorin bankar*:** Banka Qendrore e Kosovës zbuloi një sulm kibernetik në vitin 2016[11] që kishte për qëllim industrinë bankare të vendit. Për të hyrë në rrjetin e bankës dhe për të marrë të dhëna të ndjeshme, sulmuesit përdorën një email phishing. Miliona euro humbën si pasojë e sulmit ndaj bankave dhe organizatave të shumta financiare në Kosovë.

⇒ ***Sulmi ndaj sektorit qeveritar:*** Qeveria e Kosovës pretendoi një sulm kibernetik në vitin 2019[12] që ishte drejtuar ndaj sistemeve të saj kompjuterike. Për të hyrë në sistem dhe për të marrë të dhëna private, sulmuesit përdorën një email phishing. Ministria e Punëve të Jashtme dhe Ministria e Punëve të Brendshme ishin ndër organizatat qeveritare që u prekën nga sulmi.

# 5. Mungesa e parametrave të edukimit për Lirinë e Internetit dhe Sulmet Kibernetike

Edukimi i të rinjve në lidhje me lirinë e internetit, sigurinë kibernetike dhe sulmet kibernetike është thelbësor për disa arsye. Së pari, të rinjtë janë përdoruesit më aktivë dhe më të shpeshtë të teknologjive digjitale, duke i bërë ata veçanërisht të ndjeshëm ndaj kërcënimeve kibernetike. Duke u ofruar atyre një edukim gjithëpërfshirës mbi sigurinë në internet, mbrojtjen e privatësisë dhe parandalimin e sulmeve kibernetike , Kosova mund t'i fuqizojë të rinjtë e saj për të lundruar në peizazhin digjital me përgjegjësi dhe besim. Ky edukim duhet të përfshijë mësimin e tyre për rreziqet që lidhen me ndarjen e informacionit personal në internet, rëndësinë e fjalëkalimeve të forta dhe përditësimeve të rregullta të softuerit, dhe njohjen e teknikave të zakonshme të sulmeve kibernetike , si phishing dhe malëare.

Së dyti, edukimi i të rinjve për sigurinë kibernetike nxit një kulturë të qëndrueshmërisë dhe mbrojtjes proaktive. Duke futur praktika të mira të higjienës kibernetike që në moshë të hershme, Kosova mund të kultivojë një brez që e kupton vlerën e mbajtjes së një mjedisi të sigurt digjital. Kjo përfshin mësimin e tyre se si të identifikojnë dhe raportojnë kërcënimet kibernetike, si dhe inkurajimin e tyre për të adoptuar sjellje etike në internet që respekton privatësinë dhe të drejtat e të tjerëve. Duke i pajisur të rinjtë me njohuritë dhe aftësitë e nevojshme, Kosova mund t'i fuqizojë ata që të bëhen qytetarë digjitalë të përgjegjshëm që kontribuojnë në mënyrë aktive për sigurinë e tyre dhe të komuniteteve të tyre.

---

[10]Ofruesi i Telekomit IPKO pëson sulm të madh DDoS. Marrë nga https://ëëë.darkreading.com/attacks-breaches/telecom-provider-ipko-suffers-major-ddos-attack/d/d-id/1339213

[11]Banka Qendrore e Kosovës goditet nga një sulm i madh kibernetik . Marre nga https://ëëë.dcaf.ch/sites/default/files/imce/ECA/M.Asllani-YoungFaces2022.pdf

[12]Qeveria e Kosovës në shënjestër të sulmeve kibernetike. Marre nga https://ëëë.bbc.com/neës/ëorld-europe-47813711

Së fundmi, edukimi mbi sigurinë kibernetike mund të shërbejë gjithashtu si një rrugë drejt punësimit dhe mundësive të karrierës në të ardhmen. Ndërsa kërkesa për profesionistë të sigurisë kibernetike vazhdon të rritet globalisht, investimi në edukimin dhe trajnimin e të rinjve në këtë fushë mund të ndihmojë në kapërcimin e hendekut të aftësive dhe të krijojë një tubacion talentesh për industrinë e sigurisë kibernetike të Kosovës. Duke ofruar kurse të specializuara, punëtori dhe programe mentorimi, Kosova mund të ushqejë interesin dhe aftësitë e individëve të rinj në fushën e sigurisë kibernetike, duke hapur dyert për shtigje karriere emocionuese dhe me kërkesa të larta.

## 6. Perspektiva gjinore në sigurinë kibernetike

Rëndësia e integrimit të perspektivës gjinore dhe promovimit të përfshirjes gjinore në fushën e sigurisë kibernetike në Kosovë nuk mund të mbivlerësohet. Aktualisht, gratë janë të nënpërfaqësuara në sektorët e teknologjisë dhe sigurisë kibernetike, gjë që jo vetëm kufizon diversitetin, por edhe pengon efektivitetin e masave të sigurisë kibernetike. Duke adresuar në mënyrë aktive këtë hendek gjinor dhe duke siguruar mundësi të barabarta për gratë, Kosova mund të shfrytëzojë potencialin e plotë të kapitalit të saj njerëzor dhe të rrisë elasticitetin e saj të sigurisë kibernetike.

Së pari, promovimi i përfshirjes gjinore në sigurinë kibernetike ndihmon në shfrytëzimin e një grupi më të gjerë talentesh dhe ekspertize. Duke i inkurajuar dhe mbështetur në mënyrë aktive gratë për të ndjekur karrierën në këtë fushë, Kosova mund të ketë qasje në një gamë të ndryshme perspektivash, njohurish dhe aftësish. Ky diversitet mendimi dhe përvoja mund të çojë në zgjidhje më gjithëpërfshirëse dhe inovative për sfidat e sigurisë kibernetike. Për më tepër, përfshirja e grave në proceset vendimmarrëse dhe rolet drejtuese brenda sektorit të sigurisë kibernetike mund të ndihmojë në formimin e politikave dhe strategjive që janë më gjithëpërfshirëse dhe më të përgjegjshme ndaj nevojave të të gjitha palëve të interesuara.

Së dyti, një qasje gjithëpërfshirëse gjinore ndaj sigurisë kibernetike mund të kontribuojë në zhvillimin e një ekosistemi digjital më elastik dhe të sigurt. Gratë mund të sjellin perspektiva dhe njohuri unike për identifikimin e dobësive dhe rreziqeve. Duke përfshirë këto pikëpamje të ndryshme, Kosova mund të rrisë aftësinë e saj për të zbuluar dhe zbutur kërcënimet kibernetike në zhvillim. Për më tepër, nxitja e një mjedisi që është mikpritës dhe mbështetës për gratë në sigurinë kibernetike mund të çojë në rritjen e bashkëpunimit, ndarjes së njohurive dhe bashkëpunimit midis profesionistëve, duke forcuar përfundimisht pozicionin e përgjithshëm të sigurisë kibernetike të kombit.

Së fundi, promovimi i përfshirjes gjinore në sigurinë kibernetike është një çështje e barazisë sociale dhe drejtësisë. Duke siguruar qasje të barabartë në arsim, trajnim dhe mundësi karriere në terren, Kosova mund të adresojë pabarazitë ekzistuese gjinore dhe të promovojë barazinë gjinore në sektorin e teknologjisë. Kjo jo vetëm që fuqizon gratë ekonomikisht, por gjithashtu sfidon stereotipet dhe normat shoqërore, duke nxitur një shoqëri më gjithëpërfshirëse dhe progresive. Këto raste nxjerrin në pah rrezikun në rritje të sulmeve kibernetike ndaj infrastrukturës jetike të Kosovës. Sulmet, të cilat synonin industri të rëndësishme si energjia, telekomunikacioni, financat dhe qeveria, patën pasoja të rënda për institucionet e sulmuara si dhe për popullatën e përgjithshme.

**Si përfundim** Kosova ka një sërë pengesash të rëndësishme për sigurinë kibernetike. Për shkak të faktit se shumë individë nuk janë në dijeni se si të mbrohen nga sulmet në internet, ekziston një problem serioz me mungesën e njohurive për sigurinë kibernetike midis konsumatorëve dhe organizatave. Kjo përkeqësohet nga korniza joadekuate ligjore dhe rregullatore e Kosovës, e cila dështon në adresimin e kërcënimeve kibernetike dhe mbrojtjen e infrastrukturës jetike.

Aftësitë e dobëta të sigurisë kibernetike të Kosovës e bëjnë gjithashtu të papërgatitur për t'iu përgjigjur sulmeve kibernetike kur ato ndodhin. Vitet e fundit, vendi ka pasur një numër sulmesh kibernetike të profilit të lartë, duke përfshirë sulme ndaj ofruesit të telekomit, bankës qendrore dhe qeverisë. Prandaj, Kosova duhet t'i japë përparësi sigurisë kibernetike dhe të marrë masa proaktive për të forcuar pozicionin e saj të sigurisë kibernetike në mënyrë që të adresojë këto çështje. Kjo përfshin rritjen e ndërgjegjësimit të publikut dhe të korporatave, përmirësimin e mjedisit ligjor dhe rregullator dhe kryerjen e investimeve në zhvillimin e aftësive të sigurisë kibernetike. Kosova mund ta bëjë këtë për të forcuar mbrojtjen e saj kundër rreziqeve në internet dhe për të garantuar sigurinë dhe sigurinë e njerëzve, ndërmarrjeve dhe infrastrukturës jetike.

Sfidat e sigurisë kibernetike me të cilat përballet Kosova janë në përgjithësi serioze, por ato nuk janë të pakapërcyeshme. Kosova mund të zvogëlojë rreziqet e paraqitura nga kërcënimet kibernetike dhe të krijojë një ekosistem digjital më të sigurt dhe më elastik për njerëzit dhe ndërmarrjet e saj me një përpjekje dhe përkushtim të përbashkët për të forcuar pozicionin e saj të sigurisë kibernetike.

## REKOMANDIMET E FOL

⇒ **Rritja e investimeve në sigurinë kibernetike:** Qeveria dhe sektori privat në Kosovë duhet të ndajnë më shumë burime dhe fonde për të përmirësuar sigurinë kibernetike. Të krijohen iniciativa financimi dhe grante posaçërisht për kërkimin, zhvillimin dhe përmirësimin e infrastrukturës në sigurinë kibernetike. Të inkurajohen bizneset, veçanërisht SME-të, që t'i japin përparësi sigurisë kibernetike në planet e tyre buxhetore dhe operacionale. Qeveria duhet gjithashtu të rrisë shpërndarjen e saj buxhetore për iniciativat e sigurisë kibernetike, duke e njohur atë si një investim kritik për sigurinë kombëtare dhe qëndrueshmërinë ekonomike.

⇒ **Nxitja e Partneriteteve Publiko-Privat:** Lehtësimi i bashkëpunimit ndërmjet qeverisë, institucioneve akademike dhe organizatave të sektorit privat për të forcuar aftësitë e Kosovës për sigurinë kibernetike. Të krijohen partneritete për të promovuar shkëmbimin e njohurive, bashkëpunimin kërkimor dhe iniciativat e përbashkëta për zhvillimin e fuqisë punëtore të sigurisë kibernetike. Të inkurajohen kompanitë private që të marrin pjesë aktive në financimin dhe mbështetjen e projekteve të kërkimit dhe zhvillimit të sigurisë kibernetike. Duke shfrytëzuar ekspertizën dhe burimet e palëve të ndryshme të interesit, Kosova mund të përshpejtojë përparimin e saj në ndërtimin e një ekosistemi të fuqishëm të sigurisë kibernetike.

## Për t'i dhënë përparësi edukimit të të rinjve në lidhje me lirinë e internetit, sigurinë kibernetike dhe sulmet kibernetike:

⇒ **Përfshirja e edukimit për sigurinë kibernetike në kurrikulën kombëtare:** Integrimi i ndërgjegjësimit për sigurinë kibernetike dhe programet e shkrim-leximit digjital në sistemin arsimor, duke siguruar që të gjithë studentët të marrin njohuritë dhe aftësitë bazë për të mbrojtur veten në fushën digjitale.

⇒ **Promovimi i fushatave ndërgjegjësuese dhe angazhimin përmes kanaleve të shumta:** Përdorimi i kanaleve të ndryshme komunikimi, duke përfshirë mediat sociale, faqet e internetit dhe njoftimet e shërbimit publik, për të rritur ndërgjegjësimin e të rinjve për rëndësinë e sigurisë kibernetike. Inkurajoni pjesëmarrjen në forume online, konkurse dhe seminare që promovojnë të mësuarit dhe bashkëpunimin në këtë fushë.

## Për të promovuar perspektivën gjinore dhe përfshirjen gjinore në sigurinë kibernetike:

⇒ **Krijimi i programeve të mentorimit dhe mbështetjes:** Krijimi i iniciativave mentorimi që bashkojnë profesionistët me përvojë në fushën e sigurisë kibernetike me gratë që aspirojnë profesionistë. Këto programe mund të ofrojnë udhëzime, mbështetje dhe mundësi rrjetëzimi, duke ndihmuar për të kapërcyer barrierat dhe për të rritur perspektivat e karrierës për gratë në sigurinë kibernetike.

⇒ **Inkurajimi i diversitetit në praktikat e rekrutimit dhe punësimit:** Inkurajimi i organizatave në sektorin publik dhe privat që të miratojnë praktika gjithëpërfshirëse të rekrutimit dhe punësimit që i japin përparësi diversitetit, përfshirë diversitetin gjinor, në fuqinë punëtore të sigurisë kibernetike. Kjo mund të përfshijë vendosjen e objektivave për përfaqësimin e grave në terren dhe zbatimin e politikave që sigurojnë procese të drejta dhe të paanshme përzgjedhjeje.

⇒ **Investimi në iniciativa arsimore dhe bursa:** Sigurimi i bursave dhe mbështetjeve financiare për gratë që ndjekin studime dhe karrierë në sigurinë kibernetike. Kjo mund të ndihmojë në zbutjen e barrierave financiare dhe rritjen e përfaqësimit të grave në programet përkatëse arsimore. Për më tepër, mbështetni iniciativat që promovojnë edukimin digjital dhe ndërgjegjësimin për sigurinë kibernetike midis vajzave që në moshë të re për të inkurajuar interesin dhe angazhimin e tyre në këtë fushë.

Duke i zbatuar këto **rekomandime,** Kosova mund të ndërmarrë hapa të rëndësishëm drejt një sektori të sigurisë kibernetike më gjithëpërfshirëse gjinore, duke nxitur diversitetin, inovacionin dhe qëndrueshmërinë përballë kërcënimeve kibernetike në zhvillim. Zbatimi i këtyre rekomandimeve do të kërkojë një përpjekje të koordinuar ndërmjet agjencive qeveritare, institucioneve arsimore, bizneseve dhe palëve të tjera të interesuara. Duke i dhënë përparësi investimeve në arsim, trajnim, kërkim dhe zhvillim, dhe infrastrukturë, Kosova mund të përmirësojë ndjeshëm aftësitë e saj të sigurisë kibernetike dhe të mbrojë më mirë peizazhin e saj digjital.

## Referenca


1. Banka Qendrore e Kosovës goditet nga një sulm i madh kibernetik . Marre nga https://ëëë.dcaf.ch/sites/default/files/imce/ECA/M.Asllani-YoungFaces2022.pdf
2. Strategjia e Sigurisë Kibernetike e Republikës së Kosovës 2019-2022. Marrë nga https://kryeministri.rks-gov.net/ëp-content/uploads/2022/10/2-Strategjia-e-Sigurise-e-Kosoves-ENG.pdf
3. Indeksi i Ekonomisë dhe Shoqërisë Digjitale (DESI) 2020: Raporti i vendit - Kosovë. Marrë nga https://digital-strategy.ec.europa.eu/en/policies/desi
4. Komisioni Europian. (2021). Indeksi i Ekonomisë dhe Shoqërisë Digjitale (DESI) 2021: Raporti i vendit - Kosovë. Marrë nga https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021
5. Agjencia Kosovare për Shoqëri Informative (AIS) (2019). Anketa mbi sigurinë kibernetike në NVM-të në Kosovë. Marrë nga https://gcscc.ox.ac.uk/files/cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf
6. Sistemi i Shpërndarjes së Energjisë Elektrike të Kosovës pëson një sulm të madh kibernetik. Marrë nga https://ëëë.crn.com.au/neës/kosovo-electricity-distribution-system-suffers-major-cyber-attack-517394
7. Qeveria e Kosovës në shënjestër të sulmeve kibernetike. Marre nga https://ëëë.bbc.com/neës/ëorld-europe-47813711
8. Barometri Kosovar i Sigurisë (BKS) 2020: Raport Hulumtues. Marrë nga https://ais-ks.org/ëp-content/uploads/2021/04/Kosovo-Security-Barometer-2020-Research-Report.pdf
9. Ligji për veprat penale të Republikës së Kosovës Nr. 04/L-082 (2013). Marrë nga http://ëëë.gjykataeap.com/repository/docs/criminal_code_of_kosovo.pdf
10. Ligji për Mbrojtjen e të Dhënave Personale i Republikës së Kosovës Nr. 04/L-032 (2010). Marrë nga https://assembly-kosova.org/Uploads/Data/Documents/Laëno06L-082_NBuSkkM44v.pdf
11. Ofruesi i Telekomit IPKO pëson sulm të madh DDoS. Marrë nga https://ëëë.darkreading.com/attacks-breaches/telecom-provider-ipko-suffers-major-ddos-attack/d/d-id/1339213
12. Ligji për Mbrojtjen e të Dhënave Personale. Marrë nga https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616&langid=2
13. Ligji për Komunikimet Elektronike. Marrë nga https://gzk.rks-gov.net/ActDetail.aspx?ActID=2851&langid=2
14. Udhëzues AKREP https://ëëë.arkep-rks.org/Home