A JANË ORGANIZATAT JOQEVERITARE TË PËRGATITURA PËR T'U MARRË ME KËRCËNIMET KIBERNETIKE?

Analizë e perceptimeve të kapaciteteve të sigurisë kibernetike në mesin e OJQ-ve në Kosovë

Autore: Donika Elshani

Gusht 2023

Mbështetur nga: USAID

Autore: Donika Elshani

Raporti i mëposhtëm është publikuar në kuadër të projektit "Shfletimi i lirë në internet" ("Greater Internet Freedom"), zbatuar nga Internews dhe BIRN Hub, përmes mbështetjes së Agjencisë së Shteteve të Bashkuara për Zhvillim Ndërkombëtar (USAID).

Ky raport në formën e tij origjinale është shkruar në gjuhën Angleze.

Mbështetur nga:

USAID

Programi
i Trendeve
të Reja
të Kërcënimeve

A JANË ORGANIZATAT JOQEVERITARE TË PËRGATITURA PËR T'U MARRË ME KËRCËNIMET KIBERNETIKE?

ANALIZË E PERCEPTIMEVE TË KAPACITETEVE TË SIGURISË KIBERNETIKE NË MESIN E OJQ-VE NË KOSOVË

Gusht 2023

PËRMBAJTJA

RRETH PROGRAMIT:

Programi Programi i Trendeve të Reja të Kërcënimeve (The Emerging Threats Programme) është projektuar si një përgjigje ndaj kërcënimeve të reja të sigurisë vendore, rajonale dhe ndërkombëtare. Qëllimi i tij kryesor është të konsolidojë dhe të ofrojë një kuptim më të mirë të kërcënimeve të reja që vazhdimisht largohen nga konceptualizimi tradicional i sfidave të sigurisë. Duke pasur parasysh shtrirjen e kërcënimeve në zhvillim që lidhen me sigurinë kibernetike dhe dezinformimin, ky program synon të ndërtojë kapacitetet e brendshme organizative për të ofruar ekspertizë të bazuar në dëshmi për të funksionalizuar përgjigjet institucionale ndaj këtyre sfidave. Hulumtimi i bazuar në dëshmi në lidhje me Programi i Trendeve të Reja të Kërcënimevee fokusohet në: infrastrukturën kritike, sigurinë kibernetike, dezinformimin dhe sfidat hibride të sigurisë. Përderisa vlerësimi(et) e nevojave, monitorimi dhe hulumtimi mbeten aktivitete themelore për t'u zhvilluar në program, QKSS synon të shfrytëzojë ekspertizën e krijuar për të rritur drejtpërdrejt kapacitetet e institucioneve dhe agjencive ekzekutive për t'iu përgjigjur në mënyrë efektive sfidave të sigurisë kibernetike dhe dezinformimit. Programi do të zhvillohet përmes:

- **Hulumtimeve më të reja të bazuara në dëshmi në lidhje me kërcënimet e reja si: siguria kibernetike, infrastruktura kritike, dezinformimi, etj.;**
- **Fushatat për ngritjen e vetëdijes dhe avokim të synuar për të përmirësuar nivelin e të kuptuarit të sfidave që lidhen me sigurinë kibernetike dhe dezinformimin në Kosovë;**
- **Mbështetje për ngritjen e kapaciteteve për institucionet dhe agjencitë ekzekutive për të zhvilluar mjete dhe strategji për të hartuar përgjigje ndaj kërcënimeve të reja.**

PËRMBLEDHJE EKZEKUTIVE

Organizatat joqeveritare në Kosovë gjithnjë e më shumë mbështeten në mjetet digjitale për të kryer punën e tyre. Nga korrespondencat online përmes aplikacioneve të ndryshme, tek ruajtja e të dhënave të rëndësishme organizative në pajisjet elektronike dhe prania në internet përmes rrjeteve sociale, OJQ-të përdorin teknologjinë për të përmirësuar komunikimin dhe për të bashkëpunuar me palët e interesuara. Megjithatë, edhe nga përfitimet e përdorimit të këtyre mjeteve digjitale na paraqiten disa sfida dhe rreziqe që, nëse nuk trajtohen, mund të cenojnë efektivitetin dhe sigurinë e OJQ-ve dhe potencialisht madje të kërcënojnë edhe vetë ekzistencën e tyre. Akterët keqdashës po përdorin gjithnjë e më shumë sferën digjitale për të kryer aktivitete keqdashëse, duke përfshirë vjedhjen e të dhënave të ndjeshme, kryerjen e krimeve financiare, përhapjen e gënjeshtrave dhe gjuhën e urrejtjes.

Qëllimi i këtij raporti është të ofrojë një analizë të përceptimeve të OJQ-ve që lidhen me kërcënimet kryesore digjitale dhe nevojës për të ndërtuar kapacitetet e sektorit joqeveritar në Kosovë për tu bërë ballë kërcënimeve kibernetike. Rapori synon të plotësojë boshllëkun ekzistues të të dhënave duke kryer një vlerësim bazë të sfidave kryesore me të cilat përballen OJQ-të për sa i përket sigurisë digjitale dhe duke identifikuar nevojat e tyre specifike për rritjen e kapaciteteve të tyre digjitale.

Raporti bazohet në një anketë të kryer midis 48 OJQ-ve për të vlerësuar kapacitetet e tyre të sigurisë kibernetike. Gjetjet tregojnë se OJQ-të në Kosovë përballen me sfida të rëndësishme sa i përket kapacitetit të tyre për të identifikuar dhe për t'iu përgjigjur kërcënimeve kibernetike. Analiza nxjerr në pah mungesën e burimeve njerëzore dhe financiare, ekspertizës dhe masave të duhura të sigurisë kibernetike brenda këtyre organizatave për t'i trajtuar në mënyrë efektive kërcënimet e mundshme digjitale në të ardhmen. Mungesa e procedurave dhe rregulloreve për të ndihmuar në drejtimin dhe udhëheqjen e menaxhimit dhe parandalimit të incidenteve kibernetike dhe mungesa e mekanizmave të reagimit ndaj incidenteve, së bashku me faktin se shumica e të anketuarve nuk kanë kryer asnjëherë ndonjë formë të vlerësimit të rrezikut në lidhje me kërcënimet digjitale, i lë OJQ-të në Kosovë plotësisht të ekspozuara ndaj një morie rreziqesh dhe dobësish që lidhen me sferën online.

Megjithëse OJQ-të duket se i përceptojnë sulmet kibernetike si një kërcënim real për mirëqenien e tyre, ato nuk janë të angazhuara në mënyrë proaktive në adresimin dhe zbutjen e këtyre rreziqeve. Gjetjet nga analiza tregojnë mungesë të kulturës së sigurisë brenda sektorit. Raporti evidenton mungesën e procedurave dhe rregulloreve për të ndihmuar në drejtimin dhe udhëheqjen e menaxhimit dhe parandalimit të incidenteve kibernetike. Raporti gjithashtu tregon se shumica e OJQ-ve të anketuara nuk kanë kryer asnjëherë ndonjë formë të vlerësimit të rrezikut në lidhje me kërcënimet digjitale. Pa një plan konkret reagimi ndaj incidenteve dhe pa individë të specializuar brenda organizatës që janë përgjegjës për të monitoruar dhe për të reaguar në rast të ndonjë kërcënimi, këto OJQ mbeten kryesisht të papërgatitura për të trajtuar çarjet e mundshme, gjë që ka të ngjarë të çojë në vonesa, konfuzion dhe reagim joadekuat ndaj incidenteve kibernetike. Së fundi, mungesa e ndërgjegjësimit të stafit, e cila rrëndohet nga mungesa e trajnimeve dhe fushatave ndërgjegjësuese, rrit rrezikun që këta individë të bëhen viktima të sulmeve të ndryshme kibernetike. Kjo jo vetëm që shkakton dëme në organizatë, por gjithashtu ndikon në mirëqenien emocionale dhe psikologjike të vetë pjesëtarëve të stafit.

HYRJE

Përderisa hapësira digjitale po bëhet një element gjithnjë e më integral i shoqërive moderne bashkëkohore, infrastruktura kritike, shërbimet qeveritare, sektori i sigurisë dhe qytetarët në përgjithësi janë gjithnjë e më shumë të varur nga rrjeti global online. Kosova ka një nga normat më të mëdha të penetrimit në internet në Evropë.Në mars të vitit 2023, fshati i fundit në Kosovë u lidh me rrjetin e internetit. Sipas raportit të Agjencisë së Statistikave të Kosovës për vitin 2022, 98 për qind e familjeve në Kosovë kanë qasje në internet dhe përdorimi i internetit është pothuajse i barabartë në shumicën e grup moshave. Rrjedhimisht, pjesa më e madhe e aktiviteteve të përditshme të njerëzve, si komunikimi, qasja në informacion, transaksionet bankare dhe blerjet kanë kaluar në sferën online.

Ashtu si çdo entitet tjetër publik ose privat në ditët e sotme, OJQ-të shfrytëzojnë vazhdimisht teknologjitë dhe platformat digjitale për të kryer një sërë aktivitetesh që lidhen me punën e tyre, duke përfshirë ndarjen e informacionit, ndërtimin e komunitetit, ngritjen e kapaciteteve, avokimin dhe mobilizimin e burimeve. Në këtë drejtim, OJQ-të në Kosovë nuk bëjnë përjashtim. Të pakta janë organizatat që ende nuk kanë krijuar prani në internet, qoftë përmes një faqe interneti të dedikuar ose faqeve në rrjete sociale. Sidomos këto të fundit janë bërë mjetet kryesore digjitale përmes të cilave organizatat joqeveritare në Kosovë lidhen me audiencën e tyre të synuar, shpërndajnë informacione dhe angazhohen në dialog kuptimplotë.

Megjithatë, derisa organizatat gjithnjë e më shumë mbështeten në mjete të reja digjitale për të kryer operacionet e tyre të përditshme, gjurma e tyre digjitale shkon duke u rritur dhe bashkë me të rritet edhe rreziku dixhital me të cilin ata janë të prirur të përballen. Kërcënimet kibernetike që prekin OJQ-të, duke përfshirë hakimet digjitale që synojnë të shkaktojnë ndërprerje operacionale, vjedhjen e të dhënave ose përhapjen e dezinformatave, jo vetëm që pengojnë operacionet e përditshme organizative dhe anëtarët e stafit të synuar, por gjithashtu rrezikojnë marrëdhëniet e OJQ-ve me komunitetet në të cilat janë të përfshirë. Kjo është veçanërisht e rëndësishme kur merren parasysh OJQ-të që punojnë me individë dhe grupe të margjinalizuara, si gratë dhe vajzat, fëmijët, viktimat/të mbijetuarit e torturës dhe traumës, personat me aftësi të kufizuara, anëtarët e komunitetit LGBTIQ+, pakicat etnike dhe individët me probleme të shëndetit mendor, ndër të tjera. Çdo ndërprerje në operacionet e tyre ose kompromet im i të dhënave të ndjeshme mund të ketë pasoja të rënda për individët që mbështeten në shërbimet e tyre.

Mjedisi i kërcënimit dixhital në Kosovë është në evoluim dhe përfshin rreziqe dhe sfida të ndryshme që prekin qytetarët, organizatat dhe aparatusin shtetëror. Kosova ka përjetuar një sërë sulmesh kibernetike që kanë pasur ndikime të rëndësishme në shumë sektorë. Së fundmi, Telekomi i Kosovës, ofruesi i shërbimeve të telekomunikacionit në vend, ka përjetuar një sulm kibernetik i cili ka rezultuar në ndërprerje të shërbimit të internetit për përdoruesit e telefonisë mobile dhe fikse. Për më tepër, ka pasur raste të sulmeve kibernetike që kanë targetuar shërbimet qeveritare, duke çuar në sfida në lidhjen me internetin dhe qasjes të kufizuar në uebsajte të caktuara qeveritare. Hapësirat digjitale, duke përfshirë platformat e mediave sociale, po përdoren gjithnjë e më shumë për bullizmin , veçanërisht duke synuar individë të cenueshëm si gratë, të rinjtë, pakicat etnike ose anëtarët e komunitetit LGBTIQ+. Së fundi, përhapja e lajmeve të rreme dhe dezinformatave ka marr përmasa të reja, veçanërisht pas ngjarjeve të rëndësishme si pandemia COVID-19 dhe pushtimi rus i Ukrainës. Informacionet nga burime jo të besueshme dhe të dyshimta gjatë pandemisë shpesh çuan në frikë, panik dhe pasiguri sociale tek qytetarët, ndërsa narrativat e mediave ruse që synojnë të minojnë shtetësinë e Kosovës janë intensifikuar që nga fillimi i luftës në Ukrainë.

METODOLOGJIA

Ekziston një mungesë e dukshme e të dhënave në lidhje me temat që lidhen me sigurinë kibernetike në Kosovë, duke përfshirë informacione se cilat janë kërcënimet kibernetike më të përhapura me të cilat përballen individët dhe organizatat, si reagojnë këta të fundit ndaj këtyre kërcënimeve dhe mekanizmat të cilat i përdorin, nëse ka të tilla, për të zbutur incidentet kibernetike.

Qëllimi i këtij raporti është të ofrojë një analizë mbi gjendjen ekzistuese të kërcënimeve kryesore digjitale dhe nevojave për ndërtimin e kapaciteteve digjitale të sektorit joqeveritar në Kosovë. Raporti synon të plotësojë boshllëkun ekzistues të të dhënave duke kryer një vlerësim fillestar të sfidave kryesore me të cilat përballen OJQ-të në drejtim të sigurisë digjitale dhe identifikimin e nevojave të tyre specifike për rritjen e kapaciteteve të tyre digjitale.

Raporti përdor një qasje sasiore të anketimit për të vlerësuar kërcënimet e përhapura kibernetike, mekanizmat e reagimit dhe nevojat për ndërtimin e kapaciteteve digjitale. Një anketë online me 43 pyetje iu shpërnda mbi 200 OJQ-ve që veprojnë në Kosovë. Lista e OJQ-ve të cilave u është shpërndarë anketa është marrë nga baza e të dhënave të CIVIKOS, një platformë që bashkon mbi 200 OJQ në Kosovë me qëllim të promovimit të bashkëpunimit dhe angazhimit.

Pyetjet e anketës u zhvilluan në bashkëpunim me një ekspert të jashtëm të teknologjisë informative dhe bazohen në një sërë treguesish universalë të matjeve të sigurisë kibernetike për OJQ-të, duke përfshirë fusha të tilla si qeverisja, zbatimi teknik i procedurave, monitorimi i sistemeve të sigurisë dhe informacionit, testimi dhe auditimi i sistemeve të sigurisë dhe informacionit, si dhe trajnimin dhe ndërgjegjësimin e stafit. Një përshkrim më i detajuar i këtyre treguesve është dhënë në seksionin vijues të raportit.

Anketa zgjati afërsisht 5 minuta për t'u plotësuar dhe përmbante një sërë llojesh pyetjesh, të tilla si po/jo, shkalla Likert dhe disa pyetje të hapura. Microsoft Formularët u përdorën si platformë anketimi në internet dhe pjesëmarrësit e morën anketën përmes email-it. Për të siguruar një shkallë më të lartë përgjigjeje, dy email-e rikujtuese iu dërguan pjesëmarrësve gjatë periudhës së anketimit. Në anketë janë përgjigjur gjithsej 48 OJQ. Shumica e tyre (92 për qind) ishin OJQ që u identifikuan si shoqata, ndërsa pjesa tjetër u identifikuan si fondacione. Këto OJQ operojnë nëpër komuna të ndryshme në Kosovë, fushëveprimi i së cilave mbulon një gamë të ndryshme fushash, duke përfshirë të drejtat e grave, mbrojtjen e fëmijëve, pajtimin ndër-etnik, fuqizimin e të rinjve, të drejtat e njeriut dhe sundimin e ligjit, mbrojtjen e mjedisit, avokimin, dhe shërbimet psikosociale dhe shëndetësore, duke i përmendur vetëm disa.

Metoda sasiore e zgjedhur për analizën e mëposhtme shërben si një hap i parë i rëndësishëm për krijimin e bazës për të kuptuar nivelin e sigurisë kibernetike dhe qëndrueshmërinë e demonstruar nga OJQ-të në Kosovë. Megjithatë, duhet theksuar se kjo metodë ka kufizimet e saj në kontekstin e këtij studimi, përkatësisht se mund të dështojë të sigurojë një pasqyrë të detajuar dhe gjithëpërfshirëse të nevojave të sigurisë kibernetike të këtij sektori. Prandaj, hulumtime shtesë janë të nevojshme për të eksploruar më në thellësi sfidat dhe temat specifike që dalin nga ky raport.

TREGUESIT E SIGURISË KIBERNETIKE PËR OJQ-TË

Seksioni në vijim ofron një pasqyrë të treguesve të sigurisë kibernetike për OJQ-të. Këta tregues kategorizohen në pesë fusha tematike, përkatësisht qeverisja, zbatimi teknik i procedurave, monitorimi i sistemeve të sigurisë dhe informacionit, testimi dhe auditimi, si dhe trajnimi dhe ndërgjegjësimi i stafit.

Qeverisja në kontekstin e sigurisë kibernetike i referohet krijimit të politikave, procedurave dhe kornizave që drejtojnë dhe qeverisin qasjen e një organizate për menaxhimin dhe zbutjen e rreziqeve kibernetike. Kjo përfshin një sërë dokumentesh dhe masash të tilla si politikat që rregullojnë përdorimin e pajisjeve dhe llogarive elektronike, procedurat për backups (kopjet rezervë) të të dhënave, mbrojtjen e informacionit të ndjeshëm, planet e reagimit ndaj incidenteve dhe procedurat për përditësimet e softuerit dhe aplikacioneve, ndër të tjera. Zbatimi teknik i procedurave të lidhura me teknologjinë informative është një tjetër aspekt i rëndësishëm i sigurimit të qëndrueshmërisë kibernetike. Ai i referohet zbatimit praktik të mekanizmave të qeverisjes së një organizate - të tilla si politikat, procedurat dhe kornizat - të cilat u mundësojnë organizatave të krijojnë mbrojtje të fuqishme dhe mekanizma reagimi kundër kërcënimeve kibernetike. Këto procedura mund të përfshijnë zbatimin e kontrolleve të qasjes (access control), mekanizmat e kodimit, softuerin antivirus dhe pajisjet e sigurimit të rrjetit.

Monitorimi i sistemeve të sigurisë dhe informacionit që posedon një organizatë është një tregues shtesë thelbësor përmes të cilit organizatat mund të zbulojnë dhe t'i përgjigjen një incidenti kibernetik në kohë dhe në mënyrë efektive. Monitorimi mund të bëhet ose duke përdorur sisteme elektronike ose duke caktuar anëtarë të stafit brenda organizatës për të mbikëqyrur këto sisteme. Për të siguruar që një organizatë ka sisteme të forta e sigurie dhe informacioni, është e rëndësishme që këto sisteme të testohen dhe auditohen shpesh. Kjo ndihmon në identifikimin e dobësive të mundshme brenda këtyre sistemeve, të cilat, nëse mbesin të pa trajtuara, mund të çojnë në shkelje të sigurisë, qasje të paautorizuar, shkelje të të dhënave, ndërprerje të shërbimit, humbje financiare, dëmtim të reputacionit dhe pasoja të tjera të dëmshme.

Së fundi, ngritja e ndërgjegjësimit dhe aktivitetet e ndërtimit të kapaciteteve në lidhje me sigurinë, në përgjithësi, dhe sigurinë kibernetike, në veçanti, janë thelbësore për nxitjen e një kulture të fortë sigurie brenda një organizate. Këto i referohen nismave organizative që kanë për qëllim edukimin e stafit mbi temat që kanë të bëjnë me sigurinë brenda organizatës. Për shembull, trajnimi i rregullt i punonjësve për çështje të lidhura me sigurinë kibernetike ndihmon për të siguruar që ata të zhvillojnë aftësitë e nevojshme për të identifikuar një sulm të mundshëm dhe për t'iu përgjigjur në përputhje me rrethanat. Përtej kësaj, trajnimet e tilla gjithashtu i mësojnë ata se pse është e rëndësishme të kujdesen për sigurinë kibernetike në një kontekst organizativ dhe çfarë është rreziku nëse ata nuk arrijnë ta bëjnë këtë.

TABELA 1 **TREGUESIT E KATEGORIZUAR TË SIGURISË KIBERNETIKE DHE PËRSHKRIMET E TYRE SIPAS FUSHËS TEMATIKE**

FUSHA TEMATIKE	TREGUESIT	PËRSHKRIMI
QEVERISJA	» Organizata ka strategji, politikë dhe/ose procedurë në formë të shkruar për sigurinë kibernetike » Organizata ka një plan/procedurë në formë të shkruar për zbutjen e rreziqeve kibernetike » Organizata ka vendosur procedura dhe staf të veçantë për trajtimin e incidenteve të sigurisë kibernetike	Krijimi i politikave, procedurave dhe kornizave që drejtojnë dhe qeverisin qasjen e një organizate për menaxhimin dhe zbutjen e rreziqeve kibernetike
ZBATIMI TEKNIK	» Organizata është e pajisur me pajisje mbrojtëse të rrjetit si firewalls dhe SMN » Organizata përdor aplikacione për mbrojtjen e kompjuterit duke përfshirë antivirus dhe SMN » Organizata implementon sisteme të kontrollit të qasjes (access control) » Organizata vendos protokolle për kodimin e të dhënave	Zbatimi praktik i mekanizmave të qeverisjes së një organizate - të tilla si politikat, procedurat dhe kornizat - të cilat i mundësojnë asaj të krijojë mbrojtje të fuqishme dhe mekanizma reagimi kundër kërcënimeve kibernetike
MONITORIMI I SISTEMEVE TË SIGURISË DHE INFORMACIONIT	» Prania e sistemeve elektronike për monitorimin e sigurisë brenda organizatës » Organizata ka staf të veçantë për monitorimin e sigurisë kibernetike	Monitorimi i sistemeve të sigurisë dhe informacionit të një organizate për të identifikuar dhe për t'iu përgjigjur një incidenti kibernetik në kohë dhe në mënyrë efektive
TRAJNIMI DHE NDËRGJEGJËSIMI I STAFIT	» Organizata kryen testime të rregullta për të vlerësuar sigurinë e sistemeve të saja elektronike » Organizata kryen auditime të rregullta të sistemeve të saja elektronike	Testimi dhe auditimi i rregullt i sistemeve të sigurisë dhe informacionit të një organizate për të identifikuar dobësitë e mundshme brenda këtyre sistemeve
TRAJNIMI DHE NDËRGJEGJËSIMI I STAFIT	» Organizata ofron trajnime/prezantime të rregullta për stafin e saj në fushën e sigurisë kibernetike	Iniciativat organizative që synojnë edukimin e stafit për praktikat më të mira, rreziqet e mundshme dhe sjelljet e përshtatshme në lidhje me sigurinë kibernetike

HISTORIKU

Zhvillimi i kornizës ligjore të sigurisë kibernetike në vend filloi në vitet e para pas pavarësisë së Kosovës në vitin 2008. Akti fillestar legjislativ i miratuar nga Kuvendi i Kosovës në vitin 2010 ishte Ligji për Parandalimin dhe Luftimin e Krimit Kibernetik, i cili shërben si gur themeli për parandalimin, zbulimin dhe penalizimin efektiv të veprave të krimit kibernetik brenda rrjetit online. Në vitet në vijim, u ratifikuan dy ligje shtesë me rëndësi të konsiderueshme për sektorin, përkatësisht Ligji për Shërbimet e Shoqërisë Informatike, i cili hyri në fuqi në vitin 2012 dhe i cili rregullon shërbimet elektronike si e-commerce, e-banking dhe e-governance, si dhe Ligjin për Përgjimin e Komunikimeve Elektronike. Ky i fundit përbën një zhvillim të rëndësishëm në fushën e sigurisë kibernetike, pasi rregullon procedurat dhe kushtet për përgjimin e komunikimeve elektronike në lidhje me procedurën penale, sigurinë kombëtare dhe sigurinë e qytetarëve të Kosovës. Ligji për Mbrojtjen e të Dhënave Personale, i cili hyri në fuqi në vitin 2019, përbën një element të rëndësishëm shtesë të kuadrit të sigurisë kibernetike. Ky ligj përcakton të drejtat, përgjegjësitë, parimet dhe masat ndështkuese në lidhje me mbrojtjen e të dhënave personale dhe privatësisë së individëve, duke rritur më tej ekosistemin e përgjithshëm të sigurisë kibernetike. Autoriteti i pavarur përgjegjës për mbikëqyrjen e zbatimit të Ligjit për Mbrojtjen e të Dhënave Personale si dhe Ligjit për Qasje në Dokumente Publike është Agjencia për Informim dhe Privatësi. Në krye të udhëheqjes së Agjencisë është Komisionerja Krenare Sogojeva-Dërmaku, e cila u zgjodh nga Kuvendi i Kosovës në qershor 2023.

Dokumenti ligjor më gjithëpërfshirës për sigurinë kibernetike në Kosovë deri më tani është Ligji për Sigurinë Kibernetike, i cili është ratifikuar nga Presidentja i Kosovës në shkurt të vitit 2023. Ligji përcakton politikat e sigurisë kibernetike, institucionet përgjegjëse për zhvillimin, zbatimin dhe promovimin e politikave të sigurisë kibernetike, rolet dhe përgjegjësitë e autoriteteve në fushën e sigurisë kibernetike dhe detyrat e subjekteve të sigurisë kibernetike. Ai gjithashtu thekson bashkëpunimin ndër-institucional, adreson parandalimin dhe luftimin e krimit kibernetik në Republikën e Kosovës dhe parasheh themelimin e Agjencisë për Siguri Kibernetike, e cila do të veprojë si mekanizmi kryesor institucional përgjegjës për propozimin dhe zbatimin e masave të sigurisë kibernetike dhe sigurimin e garancive të përgjithshme në fushën e sigurisë kibernetike në vend.

Në nivel politikash, instrument kyç shtesë që udhëzon përpjekjet e sigurisë kibernetike në Kosovë është edhe Strategjia Shtetërore për Sigurinë Kibernetike Plani i Veprimit 2016-2019, tashmë i vjetërsuar. Strategjia u vendos për të "siguruar një mjedis të sigurt të hapësirës kibernetike duke minimizuar dhe parandaluar kërcënimet kibernetike në bashkëpunim me partnerët kombëtarë dhe ndërkombëtarë". Katër objektivat strategjike përmes të cilave trajtohet siguria kibernetike në këtë dokument janë mbrojtja e infrastrukturës kritike të informacionit, zhvillimi institucional dhe ngritja e kapaciteteve, nxitja e partneriteteve publike dhe private, reagimi ndaj incidenteve dhe bashkëpunimi ndërkombëtar. Gjithashtu, përmes kësaj strategjie u krijua pozita e Koordinatorit Kombëtar për Sigurinë Kibernetike dhe Këshilli Shtetëror për Sigurinë Kibernetike, me qëllim të forcimit të përfshirjes dhe koordinimit të shumë palëve në lidhje me sigurinë në këtë sferë.

Megjithatë, ende ekzistojnë sfida të rëndësishme kur bëhet fjalë për zbatimin e kuadrit ligjor për sigurinë kibernetike. Përderisa miratimi i Ligjit për Sigurinë Kibernetike është një hap i parë pozitiv drejt krijimit të një kuadri gjithëpërfshirës të sigurisë kibernetike, progres i kufizuar drejt

zbatimit të dispozitave kryesore të këtij ligji, siç është funksionalizimi i Agjencisë për Siguri Kibernetike në kuadër të Ministrisë së Punëve të Brendshme, i cili synon të shërbejë si autoriteti qendror për koordinimin dhe mbikëqyrjen e përpjekjeve të sigurisë kibernetike, pengon efektivitetin e tij. Për më tepër, Strategjia aktuale e Sigurisë Kibernetike dhe Plani i Veprimit 2016-2019 është i vjetërsuar. Draft Strategjia e re për Sigurinë Kibernetike 2023-2027 i është nënshtruar procesit të konsultimit publik dhe tani është në pritje të miratimit nga qeveria. Konsideratat minimale lidhur me çështjet e sigurisë kibernetike në Strategjinë e Sigurisë së Kosovës të ratifikuar së fundi për 2022-2027 janë shqetësuese, pasi ajo ngre shqetësime për nivelin e prioritetit që i jepet këtij aspekti thelbësor të sigurisë në vend.

Në mungesë të mekanizmave shtetëror për t'u mbështetur në rast incidentesh në sferën digjitale, individët, organizatat dhe bizneset shpesh duhet të mbështeten në burimet e tyre për t'iu përgjigjur çështjeve të lidhura me sigurinë kibernetike. Për më tepër, për shkak të mungesës së përgjithshme të ndërgjegjësimit publik mbi këtë temë, individët dhe organizatat shpesh dështojnë të investojnë në mënyrë proaktive në masat parandaluese. Në vend të kësaj, ata reagojnë ndaj incidenteve vetëm pasi ato të kenë ndodhur tashmë.

GJETJET KRYESORE

Seksioni i mëposhtëm ofron një përmbledhje të gjetjeve kryesore që dalin nga përgjigjet e anketës online të mbledhura në kuadër të këtij studimi. Ai vë në pah disa nga trendet, modelet dhe tendencat e përgjithshme brenda mostrës së OJQ-ve që morën pjesë në studim.

Për sa i përket madhësisë organizative, shumica e OJQ-ve (71 përqind) kanë treguar se kanë ndërmjet 1-10 individ të punësuar, 25 përqind kanë treguar se kanë 11-30 individ të punësuar dhe 14 përqindshi i mbetur kanë deklaruar se kanë 31 ose më shumë individ të punësuar. Nga gjithsej 48 OJQ që iu përgjigjën anketës, vetëm tetë raportuan se nuk kishin uebfaqe zyrtare funksionale. Megjithatë, gjashtë nga OJQ-të përmendën se përdorin platformat e mediave sociale, duke përfshirë Facebook dhe Instagram, si mjete për të komunikuar dhe për t'u përfshirë me audiencën e tyre të synuar. Seti i plotë i pyetjeve të anketës mund të gjendet në Aneksin 1.

Sipas përgjigjeve të anketës, shumica e OJQ-ve shprehën shqetësim për rreziqet e sigurisë kibernetike me të cilat përballet sektori joqeveritar në Kosovë në tërësi. Nga të gjithë të anketuarit, 44 për qind treguan se OJQ-të janë të rrezikuara ose shumë të rrezikuara nga sulmet kibernetike, ndërsa 33 përqind deklaruan se ato janë deri diku të rrezikuara. Megjithatë, kur u pyetën për rëndësinë e perceptuar të sigurisë kibernetike midis OJQ-ve në përgjithësi, shumica e tyre (58 përqind) deklaruan se siguria kibernetike konsiderohet pak ose aspak e rëndësishme. Çuditërisht, asnjë nga të anketuarit nuk tregoi se OJQ-të e shohin sigurinë kibernetike si një çështje shumë të rëndësishme organizative. Për më tepër, shumica e OJQ-ve (83 përqind) raportuan se nuk kanë qenë kurrë në shënjestër të një sulmi kibernetik në të kaluarën. Ata që kishin qenë objektiv i sulmeve të tilla në të kaluarën (17 përqind) cituan lidhur me dëmet e ndryshme që u janë shkaktuar, duke përfshirë vjedhjen financiare përmes bankingut online, humbjen e të dhënave, ndërprerjet e faqeve në internet, hakerimin e llogarisë së rrjeteve sociale dhe humbjen e kontakteve dhe dokumenteve të rëndësishme. Implikimet e këtyre gjetjeve duket se qojnë drejt një skenari ku OJQ-të njohin realitetin e kërcënimeve kibernetike, megjithatë numri i kufizuar i tyre që kanë përjetuar sulme kibernetike në të kaluarën mund të kontribuojë në nënvlerësimin e rëndësisë së sigurisë kibernetike brenda këtyre organizatave. Në thelb, kjo sygjeron që OJQ-të mund të kuptojnë rëndësinë e investimit në qëndrueshmërinë e sigurisë kibernetike vetëm pasi të jenë përballur me sfidat aktuale, dhe jo në mënyrë proaktive si një masë parandaluese.

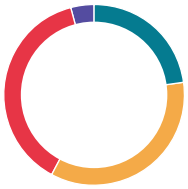
TABELA 2 **RREZIQET E SIGURISË KIBERNETIKE DHE PËRCEPTIMI I RËNDËSISË SË KËSAJ ÇËSHTJEJE NË MESIN E OJQ-VE TË ANKETUARA**

Sa janë të rrezikuara OJQ-të në Kosovë nga sulmet kibernetike?

Aspak të rrezikuara	4%
Disi të rrezikuara	33%
Pak të rrezikuara	19%
Shumë të rrezikuara	8%
Të rrezikuara	36%

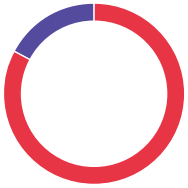
Sa i kushtojnë rëndësi OJQ-të në Kosovë sigurisë kibernetike të sistemeve që i posedojnë dhe mbrojtjes së shënimeve të cilat i trajtojnë?

Aspak 23%
Pak 35%
Deri diku 38%
I kushtojnë rëndësi 4%



A ka qenë OJQ-ja juaj ndonjëherë cak i ndonjë sulmi kibernetik në të kaluarën?

Jo 83%
Po 17%



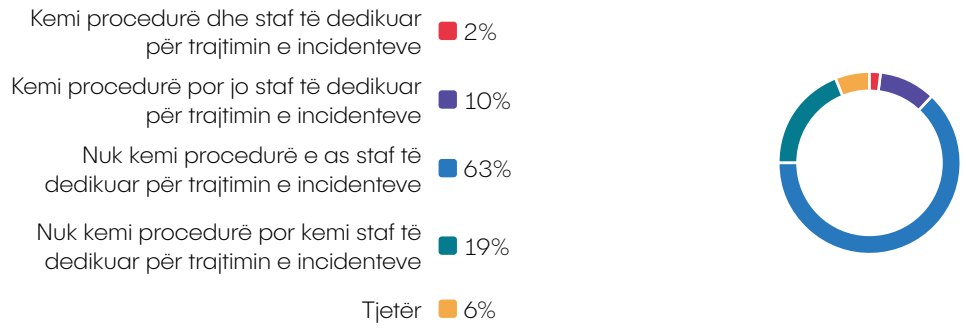
Nga 48 OJQ-të që iu përgjigjën anketës, 50 përqind deklaruan se nuk kanë ndonjë politikë, procedurë apo rregullore në fuqi që udhëzon ose rregullon qasjen e tyre për menaxhimin dhe zbutjen e rreziqeve kibernetike. Ndër OJQ-të që treguan se kishin politika, procedura ose rregullore në zbatim, 58 përqind raportuan se kishin midis 1-3 masa të tilla, ndërsa të anketuarit e mbetur raportuan se kishin 4 ose më shumë. Tre politikat e përmendura më shpesh përfshinin procedurat për krijimin e backup (kopjeve rezervë) të të dhënave, politikat për sigurinë fizike të informacionit të ndjeshëm (përfshirë përdorimin e kabineteve të skedarëve të mbyllur me dry, si dhe politikat për shkatërrimin ose asgjësimin e të dhënave të ndjeshme. Kur bëhet fjalë për reagimin ndaj incidentit, shumica e të anketuarve (62 përqind) treguan se nuk kanë një procedurë të caktuar për trajtimin e incidenteve kibernetike, e as nuk kanë ndonjë të punësuar të veçantë në mesin e stafit përgjegjës për këtë detyrë. Në mesin e të anketuarve të mbetur, 19 përqind deklaruan se ata kanë caktuar me detyrë anëtarë të stafit përgjegjës për reagimin ndaj incidentit pavarësisht se nuk kishin një procedurë formale në fuqi. Nga ana tjetër, 10 përqind deklaruan se ata kanë një procedurë për reagim ndaj incidentit, por nuk kanë anëtarë të stafit të caktuar posaçërisht për këtë detyrë. Vetëm 2 përqind e OJQ-ve që morën pjesë në këtë studim raportuan se kishin një procedurë të veçantë dhe anëtarë të stafit të caktuar me detyrë për të reaguar ndaj incidentit. Ajo që na lë të kuptojmë nga këto gjetje është se nëse shumica e OJQ-ve të anketuara do të binin viktimë e një sulmi kibernetik në të ardhmen e afërt, ato do të ishin kryesisht të papërgatitura për ta trajtuar situatën në mënyrë të menjëhershme dhe efektive, gjë që mund të çonte në pasoja potencialisht shkatërruese dhe humbje të konsiderueshme për vetë organizatën.

Një shumicë dërrmuese e të anketuarve, konkretisht 92 përqind, deklaruan se ata kurrë nuk kanë zhvilluar një vlerësim të rrezikut për sigurinë kibernetike. Me fjalë të tjera, këto organizata nuk kanë identifikuar kurrë kërcënimet dhe dobësitë e mundshme në sistemet e tyre dhe asetet e informacionit që mund t'i ekspozojnë ato ndaj sulmeve kibernetike ose shkeljeve të të dhënave. Vetëm 38 përqind e të anketuarve në studim treguan se ata kanë kryer një inventarizim të aseteve, duke përfshirë sistemet elektronike, dhe kanë identifikuar dhe vlerësuar dobësitë e pajisjeve elektronike në pronësi të organizatës së tyre. Për më tepër, vetëm 19 përqind e të anketuarve të studimit deklaruan se përdorin sisteme elektronike për të pasur qasje në informacione të ndjeshme, ndërsa vetëm 17 përqind e tyre raportuan se kishin zbatuar masa

të kontrollit të qasjes (access control). Shumica e të anketuarve (71 përqind) qasen në sistemet elektronike brenda organizatës përmes një faktori (vetëm me fjalëkalim), në vend të qasjes përmes dy apo më shumë faktorëve. Kjo gjetje vë në pah se siguria e sistemeve elektronike të OJQ-ve të anketuara është relativisht e dobët dhe e cenueshme, duke i bërë ato më të ndjeshme ndaj qasjeve të paautorizuara përmes thyerjeve të fjalëkalimeve ose sulmeve të tjera të ngjashme. Vetëm 11 përqind e OJQ-ve të anketuara raportuan se përdorin protokolle për të koduar të dhënat që barten përmes rrjetit pa tel dhe ruhen në pajisjet elektronike brenda organizatës së tyre. Një trend pozitiv që tregon për një qasje më proaktive për rritjen e sigurisë kibernetike të sistemeve dhe aseteve elektronike është se një pjesë e konsiderueshme e OJQ-ve të anketuara (60 përqind) raportuan se përdorin aplikacione për mbrojtjen kundër malware (program i dëmshëm për kompjuter) në sistemet e tyre elektronike, duke përfshirë kompjuterët, laptopët, tabletët dhe pajisje të tjera. Për më tepër, 40 nga 48 OJQ-të e anketuara treguan se përdorin një program antivirus për të mbrojtur veten gjatë shfletimit në internet.

TABELA 3 GATISHMËRIA PËR T'U BËRË BALLË SULMEVE KIBERNETIKE NË MES TË OJQ-VE TË ANKETUARA

A keni ndonjë procedurë se si trajtohen incidentet brenda OJQ-së tuaj dhe a keni ekip të dedikuar për të trajtuar incidentet?

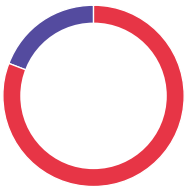


A keni bërë ndonjëherë vlerësimin e rrezikut nga sulmet kibernetike në OJQ-në tuaj?

A keni bërë ndonjëherë inventarizimin e aseteve (sistemeve elektronike)?

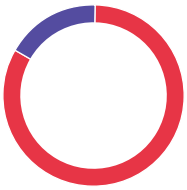
A përdorni në OJQ-në tuaj sisteme elektronike për të kontrolluar qasjen në informatat e ndjeshme?

Jo 81%
Po 19%



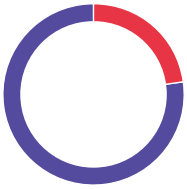
A keni në OJQ-në tuaj sisteme elektronike për përcaktimin e nivelit te qasjes (Access control) nëpër pajisje elektronike, informata, etj?

Jo 83%
Po 17%



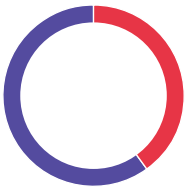
Çfarë metoda përdorni për qasjen në sistemet elektronike? (Ju lutem rrethoni përgjigjen)

Përmes më shumë faktorëve (përveç fjalëkalimit përdorni edhe smart-kartela, kodi përmes SMS, two-factor authentication, etj) 29%
Përmes një faktori (vetëm me fjalëkalim) 71%



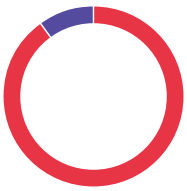
A përdorni aplikacione për mbrojtje nga malware (virus, worm, etj) në sistemet elektronike (kompjuterë, laptop, tablet, etj.) të OJQ-së tuaj?

Jo 40%
Po 60%



A përdorni protokolle për enkriptimin e shënimeve që barten përmes rrjetit pa tela?

Jo 90%
Po 10%



Përgjigjet e anketës në lidhje me statusin e licencimit të aplikacioneve të përdorura nga OJQ-të ishin pothuajse të ndara në mënyrë të barabartë. Përafërsisht 48 përqind e të anketuarve u shprehën se aplikacionet që përdorin janë të licencuara, ndërsa 52 përqindëshi i mbetur deklaruan se aplikacionet nuk janë të licencuara. Përdorimi i softuereve të licencuara brenda organizatave është shumë i rëndësishëm, pasi ndihmon OJQ-të të ruajnë besueshmërinë e tyre, të mbrojnë të dhënat e ndjeshme dhe të shmangin çështjet ligjore që mund të pengojnë funksionimin e tyre. Shumica e OJQ-ve (77 përqind) deklaruan se nuk përdorin teknologji, si VPN-in, për të mbrojtur të dhënat e magazinuara në sistemet elektronike të organizatës së tyre gjatë qasjes në distancë nga jashtë nëpërmjet internetit. 98 përqind te të anketuarve deklaruan se nuk kanë sisteme elektronike ose aplikacione të krijuara posaçërisht për menaxhimin dhe monitorimin e sigurisë kibernetike brenda OJQ-së së tyre. Asnjëra nga OJQ-të e anketuara nuk ka kryer një auditim të brendshëm të procedurave dhe sistemeve të mbrojtjes kibernetike, dhe vetëm njëra nga 48 OJQ-të i është nënshtruar një auditimi të jashtëm të sistemeve të saj elektronike në të kaluarën. Shumicës së OJQ-ve (65 përqind) u mungon stafi i veçantë përgjegjës për menaxhimin dhe monitorimin e sigurisë kibernetike brenda organizatave të tyre, dhe ata as nuk mbështeten në burime të jashtme për këtë detyrë. Mungesa e sistemeve dhe stafit përgjegjës për menaxhimin dhe monitorimin e sigurisë kibernetike është shqetësuese, pasi i lë këto OJQ plotësisht të ekspozuara ndaj një sërë rreziqesh dhe dobësish kibernetike. Kërcënimet kibernetike janë gjithmonë në evoluim, prandaj të kesh sisteme dhe staf të veçantë për të mbikëqyrur dhe monitoruar masat e sigurisë është thelbësore për të qëndruar një hap përpara shkeljeve dhe sulmeve të mundshme.

Është interesante se në mesin e OJQ-ve që deklaruan se kanë staf të veçantë, një gjetje domethënëse është se ata deklaruan se organizatat e tyre nuk ofrojnë trajnim profesional për këta anëtarë të stafit në fushën e sigurisë kibernetike. Asnjëra nga OJQ-të e anketuara nuk ka ofruar trajnime për të gjithë anëtarët e stafit të tyre në fushën e sigurisë kibernetike. Për më tepër, vetëm 2 OJQ kishin organizuar fushata ndërgjegjësuese ose prezantime për anëtarët e stafit të tyre për rreziqet e sulmeve kibernetike. Kjo tregon lidhur me mungesën e kulturës së sigurisë brenda këtyre organizatave, ku një sulm mund të ketë efekte shumëfishuese jo vetëm mbi vetë OJQ-në, por edhe për stafin e saj, duke përfshirë mirëqenien e tyre fizike dhe emocionale.

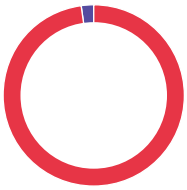
TABELA 4 GATISHMËRIA PËR T'U BËRË BALLË SULMEVE KIBERNETIKE NË MES TË OJQ-VE TË ANKETUARA (VAZHDIM)

A i keni te licencuara aplikacionet qe i përdorni në OJQ-në tuaj?

Nëse ka nevojë për qasje në shënimet që ruhen në sistemet elektronike të OJQ-së tuaj prej distance (nga jashtë përmes internetit - remote), a përdorni teknologji për mbrojtjen e këtyre shënimeve gjatë transportimit(VPN)?

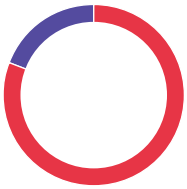
A keni në OJQ-në tuaj sisteme elektronike/aplikacione për menaxhimin dhe monitorimin e sigurisë kibernetike?

Jo 98%
Po 2%



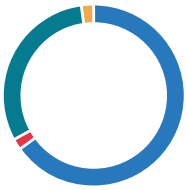
A keni bërë ndonjëherë auditim te jashtëm të sistemeve të mbrojtjes nga sulmet kibernetike për të identifikuar dobësitë në këto sisteme?

Jo 81%
Po 19%



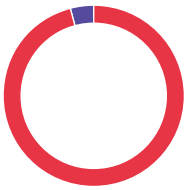
A keni në OJQ-në tuaj staf/punëtor të dedikuar dhe përgjegjës për menaxhimin dhe monitorimin e sigurisë kibernetike apo këtë e realizoni përmes resurseve të jashtme?

Asnjëra 65%
Kemi staf të dedikuar 2%
Përmes resurseve të jashtme 31%
Të dyja 2%



A keni organizuar kampanja/prezantime për stafin për ndërgjegjësimin e tyre rreth rrezikut nga sulmet kibernetike?

Jo 96%
Po 4%



REKOMANDIMET

Për të adresuar sfidat e identifikuara më lartë, është thelbësore që OJQ-të në Kosovë, pavarësisht fushëveprimit të tyre, ta marrin seriozisht sigurinë kibernetike dhe të zbatojnë rekomandimet e mëposhtme:

- **Investimi në sigurinë kibernetike duhet të jetë prioritet për OJQ-të, por nuk duhet të jetë i kushtueshëm. Ekzistojnë burime të ndryshme në dispozicion që janë me kosto efektive ose plotësisht falas, të cilat ata mund t'i përdorin për të zhvilluar dhe përmirësuar masat e tyre të sigurisë kibernetike.** Një burim i tillë është Manuali i Sigurisë Kibernetike të QKSS për Organizatat e Shoqërisë Civile në Kosovë, një udhëzues gjithëpërfshirës i përshtatur posaçërisht për nevojat e OJQ-ve në Kosovë. Manuali ofron këshilla praktike, udhëzime hap pas hapi dhe praktika të mira për zbatimin e masave efektive të sigurisë kibernetike. Me pak kohë, përpjekje dhe burime të investuara në sigurinë kibernetike, organizatat e shoqërisë civile mund të krijojnë një shteg të gjatë në forcimin e mbrojtjes së tyre dhe ndaj sulmeve digjitale.

- **Komuniteti i donatorëve duhet të rrisë mbështetjen dhe përpjekjet e tyre të bashkëpunimit me OJQ-të për të trajtuar në mënyrë efektive çështjen e sigurisë kibernetike.** Kjo mund të përfshijë forma të ndryshme ndihme, duke përfshirë burimet financiare të dedikuara për iniciativat e sigurisë kibernetike, qasjen në ekspertizë të specializuar në këtë fushë dhe ofrimin e programeve të trajnimit të përshtatura për sfidat unike me të cilat përballen OJQ-të.

- **OJQ-të duhet të jenë më të zëshme dhe proaktive në avokimin e sigurisë digjitale.** Për shkak se të gjitha OJQ-të janë ndjeshëm të prirura të jenë cak i sulmeve kibernetike - pavarësisht nga fushëveprimi i tyre - ato duhet t'i japin përparësi kësaj çështjeje dhe të luajnë një rol aktiv në rritjen e ndërgjegjësimit për kërcënimet kibernetike, qofshin ato hakime të sigurisë, shkelje të të dhënave, operacione dezinformimi apo çdo formë tjetër sulmi online. Duke shfrytëzuar platformat e ndryshme online dhe offline që OJQ-të përdorin në punën e tyre të përditshme, ato mund të angazhohen me grupet e tyre të synuara dhe audiencën më të gjerë për çështje që kanë të bëjnë me sigurinë digjitale dhe të drejtat digjitale.

ANEKSI 1.

LISTA E PYETJEVE TË ANKETËS

PYETËSORI PËR NIVELIN E SIGURISË KIBERNETIKE NË MESIN E OJQ-VE NË REPUBLIKËN E KOSOVËS

1. Emri i organizatës që ju e përfaqësoni:

2. Qyteti ku operon organizata juaj:

3. Viti kur është themeluar organizata juaj

4. Lloji i organizatës joqeveritare (OJQ):

a. Institut
b. Fondacion
c. Shoqatë

5. Fushëveprimi i punës së organizatës suaj:

6. Numri i punonjësve në organizatën tuaj:

a. 1-10
b. 11-30
c. 31-60
d. 61+

7. Uebfaqja e organizatës suaj:

8. Ju lutemi, përgjigjuni pyetjes si më poshtë duke zgjedhur një nga opsionet e ofruara:

Sa janë të rrezikuara OJQ-të në Kosovë nga sulmet kibernetike?

a. Aspak
b. Pak
c. Deri diku
d. Të rrezikuara
e. Shumë të rrezikuara

9. A ka qenë ndonjëherë OJQ-ja juaj objektiv i një sulmi kibernetik në të kaluarën?

a. Po
b. Jo

10. Nëse po, cili ishte dëmi i shkaktuar nga ky sulm?

11. Ju lutemi përgjigjuni pyetjes si më poshtë duke zgjedhur një nga opsionet e dhëna:

Sa rëndësi i kushtojnë OJQ-të e Kosovës sigurisë kibernetike të sistemeve që posedojnë dhe ruajtjes së të dhënave që ata menaxhojnë?

a. Aspak
b. Pak
c. Deri diku
d. E rëndësishme
e. Shumë e rëndësishme

12. Ju lutemi përgjigjuni me 'po' ose 'jo' pyetjeve të mëposhtme:

A keni kryer ndonjëherë një vlerësim të rrezikut për sulmet kibernetike në OJQ-në tuaj?

a. Po
b. Jo

A keni bërë ndonjëherë një inventarizim të aseteve (sistemet elektronike) në OJQ-në tuaj?

a. Po
b. Jo

A keni identifikuar ose vlerësuar ndonjëherë dobësitë e pajisjeve elektronike në pronësi të organizatës suaj?

a. Po
b. Jo

A përdorni sisteme elektronike në OJQ-në tuaj për të kontrolluar qasjen në informacione të ndjeshme?

a. Po
b. Jo

A keni sisteme elektronike në OJQ-në tuaj për përcaktimin e nivelit të kontrollit të qasjes për pajisjet elektronike, informacionin etj.?

a. Po
b. Jo

13. Cilën nga të mëposhtmet i posedon OJQ-ja juaj? (Kontrollo të gjitha opsionet e aplikueshme)

a. Parimet, procedura ose rregullore të shkruara të sigurisë kibernetike
b. Parimet, procedurat ose rregulloret për krijimin e fjalëkalimeve, gjatësinë minimale të fjalëkalimit, kompleksitetin e fjalëkalimit dhe frekuencën e ndryshimit të fjalëkalimit
c. Parimet, procedurat ose rregulloret për përditësimin e softuerit dhe aplikacioneve të përdorura nga OJQ-ja juaj
d. Parimet, procedurat ose rregulloret për përdorimin e pajisjeve celulare (tableta, telefona të menqur, etj.
e. Procedura për krijimin e back-up (kopjeve rezervë) të të dhënave tuaja
f. Procedura për rinovimin e të dhënave në rast të një sulmi kibernetik ose fshirjes ose humbjes aksidentale/të qëllimshme të këtyre të dhënave
g. Parimet për sigurinë fizike të informacionit të ndjeshëm (kabineteve të skedarëve të mbyllur me dry, etj.)
h. Parimet për shkatërrimin ose asgjësimin e të dhënave të ndjeshme pas përfundimit të përdorimit të tyre
i. Plan konkret se si të reagohet në rast incidentesh, qofshin ato të natyrës kibernetike apo fizike
j. Procedura për raportimin e jashtëm të rasteve kur ka dyshime për një incident kibernetik
k. Procedura për identifikimin dhe regjistrimin e individëve që vizitojnë fizikisht ambientet e OJQ-së tuaj
l. Asnjërën nga të sipërmet

14. Nëse OJQ-ja juaj ka parime, procedura ose rregullore të sigurisë kibernetike, a u komunikohen ato të gjithë punonjësve të organizatës?

a. Po
b. Jo
c. OJQ-ja nuk ka asnjë politikë, procedurë apo rregullore të sigurisë kibernetike

15. A i përditësoni politikat, procedurat ose rregulloret që i keni cekur në pyetjen e mëparshme?

a. Po
b. Jo
c. OJQ-ja nuk ka asnjë politikë, procedurë apo rregullore të sigurisë kibernetike

16. Nëse po, sa shpesh i përditësoni ato?

17. A keni ndonjë procedurë se si trajtohen incidentet brenda OJQ-së tuaj dhe a keni një ekip të veçantë për të trajtuar këto incidente?

a. Ne kemi procedura dhe një staf të veçantë për trajtimin e incidenteve
b. Ne kemi procedura por jo staf të veçantë për trajtimin e incidenteve
c. Ne nuk kemi procedura, por kemi staf të veçantë për trajtimin e incidenteve
d. Ne nuk kemi një procedurë për trajtimin e incidenteve, e as nuk kemi staf të veçantë
e. Tjera

18. A keni ndonjë partneritet me organizata apo kontraktorë të tjerë që janë të përfshirë në procesimin e të dhënave të ndjeshme të OJQ-së tuaj?

a. Po
b. Jo

19. Nëse po, a keni një procedurë në OJQ-në tuaj për verifikimin dhe monitorimin e këtyre partnerëve/kontraktorëve në lidhje me sigurinë kibernetike?

a. Po
b. Jo

20. Gjatë orarit të punës, punonjësit në OJQ-në tuaj kanë qasje të plotë në pajisjet si më poshtë:

a. Laptopë/kompjuterë personalë
b. Laptopë/kompjuter pune
c. Të dyja
d. Tjera

21. Çfarë metoda përdorni për të pasur qasje në sistemet elektronike (Ju lutemi zgjidhni një nga të mëposhtmet)

a. Përmes metodës me një faktor (vetëm fjalëkalim)
b. Përmes metodës me shumë faktorë (përveç fjalëkalimit, duke përdorur metoda të tilla si kartela të mençura, SMS kodet, vërtetësisë me dy faktorë, etj.)

22. Ju lutemi përgjigjuni me "Po" ose "Jo" në pyetjet e mëposhtme:

A përdorni aplikacione për mbrojtje kundër malware (program i dëmshëm për kompjuter) (viruseve, krimbave, etj.) në sistemet elektronike (kompjuterë, laptopë, tableta, etj.) të OJQ-së tuaj?

a. Po
b. Jo

A përdorni protokolle për vërtetësinë e përdoruesve që hyjnë në këtë rrjet?

a. Po
b. Jo

A përdorni protokolle për kodimin e të dhënave të transmetuara përmes rrjetit?

a. Po
b. Jo

A përdorni protokolle për kodimin e të dhënave të magazinuara në pajisjet elektronike (serverët) në OJQ-në tuaj?

a. Po
b. Jo

Po A përdorni protokolle për kodimin e të dhënave të magazinuara në kompjuterët/ laptopët e punonjësve të OJQ-së tuaj?

a. Po
b. Jo

23. Cilat aplikacione i përdorni për komunikim zyrtar në OJQ-në tuaj?

a. Email zyrtar i OJQ-së (me domenin e OJQ-së)
b. Microsoft Teams
c. Zoom aplikacioni
d. Email personal të punonjësve
e. Tjera

24. Çfarë teknologjie përdorni për sigurinë në internet? (kontrollo të gjitha ato që aplikohen)

a. Programet Antivirus
b. Programet Firewall
c. Programet SMN
d. Pajisjet Firewall
e. Tjera

25. A janë të licencuara aplikacionet që përdorni në OJQ-në tuaj?

a. Po
b. Jo

26. Nëse ekziston nevojë për qasje nga distanca në të dhënat e magazinuara në sistemet elektronike të OJQ-së tuaj (nga jashtë nëpërmjet internetit - qasje në distancë), a përdorni teknologjinë për të mbrojtur këto të dhëna gjatë transportit (VPN)?

a. Po
b. Jo

27. A keni sisteme/aplikacione elektronike në OJQ-në tuaj për menaxhimin dhe monitorimin e sigurisë kibernetike?

a. Po
b. Jo

28. A keni staf ose personel të veçantë përgjegjës për menaxhimin dhe monitorimin e sigurisë kibernetike brenda OJQ-së tuaj, apo e zgjidhni këtë nëpërmjet burimeve të jashtme?

a. Ne kemi staf të veçantë
b. Përmes burimeve të jashtme
c. Të dyja
d. Tjera

29. Kush është përgjegjës për sigurinë kibernetike dhe sigurinë e të dhënave në OJQ-në tuaj? Si përcaktohet kjo përgjegjësi (p.sh., përmes dokumenteve, politikave)? (Kontrollo të gjitha ato që aplikohen)

a. Stafi i veçantë i emëruar përmes një procedure
b. Menaxhmenti është përgjegjës, sipas procedurës
c. Ne nuk kemi një procedurë që përcakton përgjegjësinë
d. Personi përgjegjës për çështjet teknike - personeli i IT-së
e. Të gjitha të mësipërmet
f. Asnjëra nga të sipërmet
g. Tjera

30. Nëse keni staf të dedikuar për menaxhimin dhe monitorimin e sigurisë kibernetike në OJQ-në tuaj, a marrin ata trajnime të rregullta profesionale në fushën e sigurisë kibernetike?

a. Po
b. Jo
c. Nuk kemi staf të veçantë

31. A ofron OJQ-ja juaj trajnime për stafin e saj në fushën e sigurisë kibernetike?

a. Po
b. Jo

32. Nëse po, sa trajnime të tilla janë ofruar në vitin e kaluar (2022)?

33. A keni organizuar fushata/prezantime për stafin për të rritur ndërgjegjësimin e tyre për rreziqet e sulmeve kibernetike ?

a. Po
b. Jo

34. Nëse Po, kur ishte hera e fundit që i organizuat ato?

35. A keni kryer ndonjëherë teste sigurie të sistemeve elektronike të OJQ-së suaj?

a. Po
b. Jo

36. Nëse po, kur ishte hera e fundit që e keni bërë këtë?

37. A keni kryer ndonjëherë një auditim të brendshëm të procedurave dhe sistemeve për mbrojtjen nga sulmet kibernetike për të identifikuar dobësitë në këto sisteme?

a. Po
b. Jo

38. Nëse po, kur ishte hera e fundit që e keni bërë këtë?

39. A keni kryer ndonjëherë një auditim të jashtëm të sistemeve të mbrojtjes nga sulmet kibernetike për të identifikuar dobësitë në këto sisteme?

a. Po

b. Jo

40. Nëse po, kur ishte hera e fundit që e keni bërë këtë?

41. A keni kryer ndonjëherë testime të stafit për të vlerësuar njohuritë e tyre për identifikimin e sulmeve kibernetike (keqdashësit- phishing)?

a. Po

b. Jo

42. Nëse po, kur ishte hera e fundit që e keni bërë këtë?

43. Sa përqind të buxhetit/fondeve investon OJQ-ja juaj në sigurinë kibernetike?

SHËNIMET

1. Ndarja dixhitale mahnitëse e Evropës, në një hartë." Big Think. 23 qershor 2023. https://bigthink.com/strange-maps/europe-digital-divide/

2. "Çdo fshat në Kosovë tani është i lidhur me internetin me brez të gjerë me shpejtësi të lartë, me mbështetjen e Bankës Botërore." Banka Botërore. https://www.worldbank.org/en/news/press-release/2023/03/21/-every-village-in-kosovo-now-connected-to-high-speed-broadband-internet-with-world-bank-support (qasur qershor 19, 2023).

3. Agjencia e Statistikave të Kosovës, Rezultatet e Anketës për Përdorimin e Teknologjisë së Informacionit dhe Komunikimit në vitin 2022. https://ask.rks-gov.net/media/7157/tik-ne-ek-familjare-2022.pdf (qasur qershor 20, 2023).

4. Lyn, Theo et al. "Teknologjitë Dixhitale dhe Shoqëria Civile". Springer. (2022): 42. https://link.springer.com/chapter/10.1007/978-3-030-91247-5_5

5. Summers, Evan. Doracak për sigurinë kibernetike për organizatat e shoqërisë civile. Instituti Kombëtar Demokratik, 2022. https://www.ndi.org/sites/default/files/%5BEnglish%5D%20Cybersecurity%20Handbook%20for%20Civil%20Society%20Organizations-compressed.pdf (qasur qershor 13, 2023).

6. "Navigimi në sigurinë kibernetike: Udhëzime për (I) profesionistët e ZKS-ve". Qendra Ndërkombëtare e Shoqërisë Civile dhe Instituti i Paqes Kibernetike (2022) https://solidarityaction.network/media/cybersecurity-guidance.pdf (qasur qershor 12, 2023).

7. "Telekomi i Kosoves, cak i sulmeve kibernetike" Radio Evropa e Lire, Shtator. 13, 2022. https://www.evropaelire.org/a/telekomi-i-kosoves-sulme-kibernetike-/32032233.html

8. Vllahiu, Emirjeta. "Kosova do të themelojë Agjencinë për Sigurinë Kibernetike në mes të sulmeve të fundit." Balkan Insight. shtator. 14, 2022. https://balkaninsight.com/2022/09/14/kosovo-to-establish-agency-for-cyber-security-amid-recent-attacks/

9. Gjocaj, Shqipe. "Squash Online Gjuha e urrejtjes." Kosova 2.0. shkurt. 25, 2022. https://kosovotwopointzero.com/en/squash-online-hate-speech/

10. Ondozi, Qerim. "Keqinformimi, dezinformimi dhe lajmet e rreme në mediat online në Kosovë". Këshilli i Mediave të Shkruara të Kosovës (2022). http://presscouncil-ks.org/wp-content/uploads/2022/09/Raporti_Keqinformimi_ENG_Final-2.pdf

11. https://balkaninsight.com/2021/09/07/kosovo-urged-to-start-countering-russian-media-disinformation/ (qasur Maj 29, 2023).

12. CIVIKOS, faqja zyrtare: http://www.civikos.net/en/background

13. "Udhëzues për qeverisjen e mirë në sigurinë kibernetike" Qendra e Gjenevës për Qeverisjen e Sektorit të Sigurisë. (2019). https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021.pdf

14. Ligji NR. 03/L për Parandalimin dhe Luftën e Krimit Kibernetik. https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2682

15. Ligji NR. 04/L-094 Për Shërbimet e Shoqërisë Informatike, https://cps.rks-gov.net/wp-content/uploads/2020/09/LAW_NO._04_L-094_ON_THE_INFORMATION_SOCIETY_SERVICES.pdf

16. Ligji NR. 05/L-030 Për Përgjimin e Komunikimeve Elektronike, https://cps.rks-gov.net/wp-content/uploads/2020/08/LAW_NO._05_L-030_ON_INTERCEPTION_OF_ELECTRONIC_COMMUNICATIONS.pdf

17. Ligji nr. 06/L-082 për mbrojtjen e të dhënave personale, https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=18616

18. Agjencia për Informim dhe Privatësisë, faqja zyrtare e internetit: https://aip.rks-gov.net/en/aip-english/

19. Ligji Nr. 08/L-173 Për Sigurinë Kibernetike, https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933

20. Vllahiu, Emirjeta. "Kosova do të themelojë Agjencinë për Sigurinë Kibernetike pas sulmeve të fundit. Balkans Insight (shtator. 14, 2022). https://balkaninsight.com/2022/09/14/kosovo-to-establish-agency-for-cyber-security-amid-recent-attacks/

21. Strategjia Kombëtare e Sigurisë Kibernetike dhe Plani i Veprimit 2016 – 2019. https://afyonluoglu.org/PublicWebFiles/strategies/Europe/Kosovo%202016-2019%20Cyber%20Security%20Strategy-EN.pdf

22. Ligji Nr. 08/L-173 Për Sigurinë Kibernetike, https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933

23. Draft Strategjia e Sigurisë Kibernetike e Kosovës 2023– 2027, https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=41780

24. Strategjia e Sigurisë së Kosovës 2022 – 2027, https://kryeministri.rks-gov.net/wp-content/uploads/2022/10/2-Strategjia-e-Sigurise-e-Kosoves-ENG.pdf

Katalogimi në botim – **(CIP)**
Biblioteka Kombëtare e Kosovës "Pjetër Bogdani"

061.2:007(496.51)(047)

Elshani, Donika
A janë organizatat joqeveritare të përgatitura për t'u marrë me kërcënimet kibernetike? : analizë e perceptimeve të kapaciteteve të sigurisë kibernetike në mesin e OJQ-ve në Kosovë / Donika Elshani. - Prishtinë : QKSS, 2023. - 27 f. : ilustr. ; 28 cm.

ISBN 978-9951-842-04-4

Rreth QKSS-së

E themeluar në prill 2008, Qendra Kosovare për Studime të Sigurisë (QKSS) është agjenci e specializuar, e pavarur dhe joqeveritare. Qëllimi primar i QKSS është të promovojë demokratizimin e sektorit të sigurisë në Kosovë dhe të përmirësojë punën kërkimore dhe avokuese në lidhje me sigurinë, sundimin e ligjit dhe bashkëpunimin rajonal dhe ndërkombëtar në fushën e sigurisë.

QKSS synon të rrisë efektivitetin e Reformës së Sektorit të Sigurisë duke mbështetur programet e këtij sektori përmes hulumtimeve, eventeve, trajnimeve, avokimit dhe këshillave të drejtpërdrejta për politikë-bërësit. Avancimi i ideve të reja dhe metodave të shkencave sociale janë gjithashtu vlerat thelbësore të qendrës. Çdo vit, QKSS publikon raporte të shumta, analiza të politikave dhe përmbledhje të politikave për çështjet që kanë të bëjnë me sigurinë. QKSS gjithashtu organizon më shumë se 200 ngjarje publike duke përfshirë konferenca, tryeza dhe debate, ligjërata në Kosovë, ku një pjesë e tyre organizohen në bashkëpunim me partnerë rajonalë dhe ndërkombëtarë. Një gamë e gjerë aktivitetesh përfshijnë hulumtimin, ngritjen e kapaciteteve, ngritjen e ndërgjegjësimit dhe avokimin.

Puna e QKSS-së mbulon një gamë të gjerë temash, duke përfshirë por pa u kufizuar në: reformën dhe zhvillimin e sektorit të sigurisë; identifikimin dhe analizimin e rreziqeve të sigurisë që lidhen me ekstremizmin, radikalizmin dhe krimin e organizuar; politikën e jashtme dhe bashkëpunimi rajonal; dhe vlerësimin e sundimit të ligjit në Kosovë.

Këtë vit QKSS shënoi 15 vjetorin e themelimit. Për më shumë detaje rreth QKSS, shihni faqet zyrtare në rrjete sociale të organizatës, të cilat mund t'i gjeni më poshtë:

qkss.org
securitybarometer.qkss.org

@KCSSQKSS
#KCSSQKSS

ISBN 978-9951-842-04-4