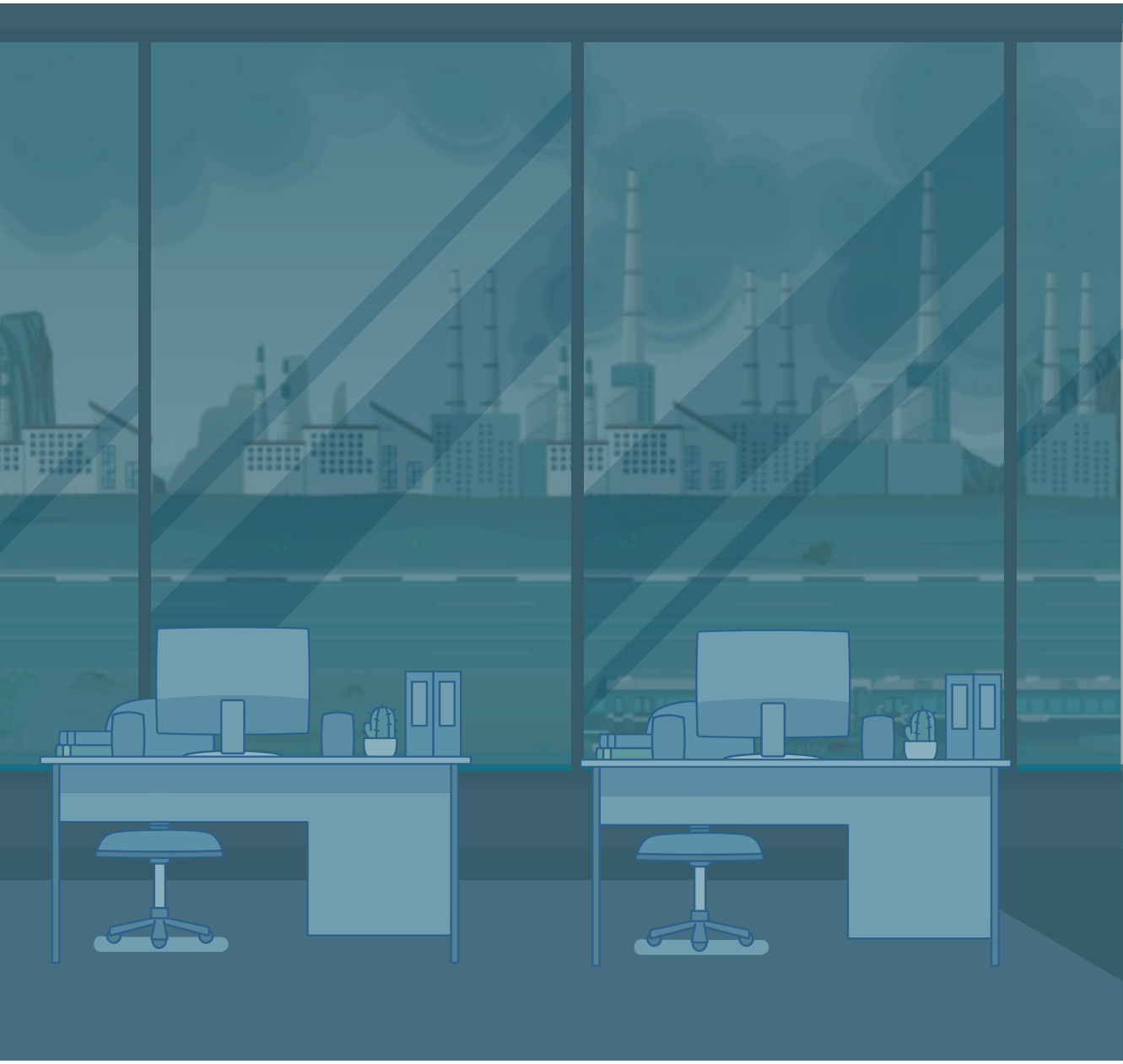
QKSS
Qendra Kosovare për Studime të Sigurisë

PROGRAMI KËRCËNIMET E REJA

RRUGA DREJT QËNDRUESHMËRISË:
Qeverisja dhe ndërtimi i kapaciteteve në Sigurinë Kibernetike dhe Infrastrukturën Kritike të Kosovës



Mars 2024

PROGRAMI KËRCËNIMET E REJA

Autor: *Chris J. Dolan*

Rreth Programit Kërcënimet e Reja

Kërcënimet e Reja (The Emerging Threats Programme) është projektuar si një përgjigje ndaj kërcënimeve në rritje të sigurisë vendore, rajonale dhe ndërkombëtare. Qëllimi i tij kryesor është të konsolidojë dhe të ofrojë një kuptim më të mirë të kërcënimeve në zhvillim 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 Programin e Kërcënimeve e reja (The Emerging Threats Programme) fokusohet në: infrastrukturën kritike, sigurinë kibernetike, dezinformimin dhe sfidat hibride të sigurisë. Përderisa vlerësimi(et) e nevojave, monitorimi dhe hulumtimi mbeten veprime 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 në zhvillim si: siguria kibernetike dhe dezinformimi;
- 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 në zhvillim.

Për më shumë informacion, na kontaktoni në: EmergingThreats@qkss.org

QKSS
Qendra Kosovare për Studime të Sigurisë

RRUGA DREJT QËNDRUESHMËRISË:
Qeverisja dhe ndërtimi i kapaciteteve në Sigurinë Kibernetike dhe Infrastrukturën Kritike të Kosovës

Mars 2024

Përmbajtja

PËRMBLEDHJE EKZEKUTIVE

Qeveria e Kosovës (QK) i ka përcaktuar si prioritete kombëtare sigurinë kibernetike dhe mbrojtjen e infrastrukturës kritike. Qeveria e Kosovës e ka nxjerr Ligjin për Sigurinë Kibernetike (LSK) dhe Ligjin për Infrastrukturën Kritike (LIK) dhe ka miratuar Strategjinë e Sigurisë së Kosovës (SSK) dhe Strategjinë e Sigurisë Kibernetike. Ajo gjithashtu e ka themeluar edhe Agjencinë për Siguri Kibernetike (ASK) e krijuar për të funksionuar si një nyjë qendrore për koordinimin e agjencive kibernetike të Qeverisë së Kosovës dhe mbrojtjen e aseteve kibernetike nëpër sektorë të ndryshëm. Përveç kësaj, Qeveria e Kosovës i ka dhënë prioritet qeverisjes dhe ndërtimit të kapaciteteve në mbrojtjen kibernetike dhe identifikimin e sektorëve kyç në infrastrukturën kritike.

Por sfidat mbeten dhe se ende shumë punë duhet të bëhen nëse Kosova dëshiron të ndërtojë qëndrueshmëri ndaj sulmeve kibernetike dhe të sigurojë sektorët e saj të infrastrukturës, veçanërisht në energji, e-qeverisje dhe telekomunikacion. Gjithnjë e më shumë njerëz në Kosovë, si dhe në të gjithë Ballkanin Perëndimor, përdorin teknologjitë e informacionit dhe komunikimit (TIK) sot si kurrë më parë, që do të thotë se do të ndodhin më shumë incidente dhe sulme kibernetike. Ku, 95% e popullatës së Kosovës ndërmjet moshës 16-74 vjeç kanë qasje të rregullt në internet dhe se mbulimi me brez të gjerë-broadband dhe telekomunikacionin 5 po shtohet për çdo vit. Kosova ka shënuar një rritje të shkeljeve dhe krimeve kibernetike, ku në shënjestër ishin telekomunikacioni, institucionet financiare dhe shërbimet e e-qeverisjes. Nga viti 2020 deri në vitin 2023, Kosova përjetoi një rritje të konsiderueshme të sulmeve malware, inxhinierisë sociale dhe ransomware, ku shumica e tyre fare e nuk janë raportuar tek autoritetet. Për më tepër, institucionet publike të Kosovës janë cak i sulmeve në baza të rregullta. Sulmet e profilit të lartë kishin në shënjestër Komisionin Qendror të Zgjedhjeve të Kosovës, Telekomin e Kosovës, dhe platformën e-Kosova. Zyra e Hetimeve të Krimeve Kibernetike në Policinë e Kosovës mban të dhëna për arrestimet dhe kapjen e kriminelëve të dyshuar kibernetikë.

Përderisa kërcënimet dhe sulmet kibernetike kundër sektorëve të infrastrukturës kritike dhe institucioneve publike të Kosovës bëhen gjithnjë e më të sofistikuara, Qeveria e Kosovës duhet të jetë e pamëshirshme dhe vigjilente në ndjekjen e koncepteve të qëndrueshmërisë përmes përpjekjeve për ndërtimin e kapaciteteve dhe lidhjen e kapaciteteve me kornizat e qeverisjes. Qeveria e Kosovës ka miratuar legjislacionin kryesor, ka hartuar dokumente udhëzuese strategjike dhe ka themeluar agjenci për të i adresuar kërcënimet kibernetike. Megjithëse qeverisja është përmirësuar dhe agjencitë kibernetike janë në funksion, ndërtimi i kapaciteteve ende mbetet një sfidë. Qeveria e Kosovës duhet të punojë me partnerët e saj ndërkombëtarë, të ndërtojë, mirëmbajë dhe zgjerojë partneritetet me sektorin dinamik privat të Kosovës dhe të promovojë edukimin dhe ndërgjegjësimin për sigurinë kibernetike.

Në vitin 2023 dhe 2024, QKSS publikoi analiza të infrastrukturës kritike dhe sigurisë kibernetike. Aty përfshihen udhëzimet për kërcënimet digjitale dhe ngritjen e kapaciteteve në OJQ, praktikat më të mira në sektorët të infrastrukturës kritike së Kosovës, modelimin e qasjeve të mbrojtjes të infrastrukturës kritike të zhvilluara nga shtetet Baltike, mbrojtja e infrastrukturës kritike të

Kosovës në një perspektivë rajonale krahasuese, përafrimi i Ligjit për Infrastrukturën Kritike me Direktivën NIS2 të Bashkimit Evropian, dhe një manual për sigurinë kibernetike për reagimin ndaj incidenteve, mbrojtjen e të dhënave dhe sigurinë në internet.

Ky raport mbështetet në vlerësimet burimeve të hapura/publike të informacionit të disponueshëm publikisht dhe në intervistat e strukturuara me palët e interesuara të Kosovës në institucionet publike dhe sektorin privat për të vlerësuar progresin në qeverisje dhe kapacitetet. Raporti analizon legjislacionin dhe kornizat qeverisëse për sigurinë kibernetike dhe infrastrukturën kritike, udhëzimet strategjike dhe operacionet dhe kapacitetet e agjencive. Raporti arrin në përfundim se nevojiten përpjekje nga e gjithë qeveria dhe të shoqëria për ta mbajtur Kosovën në rrugën e qëndrueshmërisë.

Gjetjet

Pozicioni i mbrojtjes kibernetike dhe kapacitetet të mbrojtjes së infrastrukturës kritike të Kosovës mbështetet në ndërtimin e një shoqërie të qëndrueshme dhe një ekonomie prosperuese, mbrojtjen e të dhënave dhe të drejtave të privatësisë dhe sigurimin e aseteve dixhitale. Por, në fakt Kosova po i ndërton kapacitetet nga themeli. Bazuar në këto vëzhgime, ky raport nxjerr gjetjet si vijojnë më poshtë:

1. **Ligjet dhe udhëzimet strategjike:** Ligji për Sigurinë Kibernetike (LSK) dhe Ligji për Infrastrukturën Kritike (LIK) si dhe Strategjia e Sigurisë së Kosovës (SSK) dhe Strategjia e Sigurisë Kibernetike janë arritje të rëndësishme legjislative që trajtojnë në mënyrë kolektive kërcënimet kibernetike, rreziqet dhe dobësitë si prioritete të sigurisë kombëtare. Themelimi i Agjencisë së Sigurisë Kibernetike është një hap i rëndësishëm drejt forcimit së pozitës dhe qëndrueshmërisë së mbrojtjes kibernetike të Kosovës.

2. **Agjencia për Siguri Kibernetike (ASK):** Përderisa arritjet legjislative, reformat dhe udhëzimet strategjike pasqyrojnë vëmendjen e Qeverisë së Kosovës në forcimin e qeverisjes në mbrojtjen kibernetike dhe ndërtimin e mbrojtjes të infrastrukturës kritike, ASK-ja duhet të marrë mbështetjen e nevojshme pasi të bëhet operacionale në mbikëqyrjen e zbatimit të politikave kibernetike dhe reagimit ndaj incidenteve. Koordinimi i centralizuar i agjencive është i nevojshëm për të siguruar që legjislacioni, udhëzimet strategjike dhe kapacitetet janë në linjë dhe se zërat e palëve kryesore të interesuara merren në konsiderim.

3. **3. Nevojat për ngritjen e kapaciteteve:** Përmirësime të vazhdueshme nevojiten për të tërhequr dhe mbajtur një fuqi punëtore eksperte kibernetike në institucionet publike, partnerët ndërkombëtarë dhe partneritetet publiko-private janë shtylla kryesore të sigurisë kibernetike dhe mbrojtjes kritike të infrastrukturës, qasja në teknologjitë dhe aplikacionet e avancuara do të nxisë të dhënat e inteligjencën lidhur me kërcënimet, skanimin e cenueshmërisë dhe zvogëlimin e rreziqeve, dhe edukimi e ndërgjegjësimi për sigurinë kibernetike janë shtyllat kryesore të qëndrueshmërisë për gjithë qeverinë dhe për gjithë shoqërinë.

Hyrje

Me Ligjin për Sigurinë Kibernetike (LSK) dhe Ligjin për Infrastrukturën Kritike (LIK) si dhe Strategjinë e Sigurisë së Kosovës (SSK) dhe Strategjinë e Sigurisë Kibernetike, Qeveria e Kosovës tani e konsideron mbrojtjen kibernetike dhe mbrojtjen e infrastrukturës kritike si prioritete të sigurisë kombëtare. Ligjet dhe udhëzimet strategjike shërbejnë si korniza qeverisëse për agjencitë përgjegjëse për sigurimin e energjisë, telekomunikacionit, e-qeverisjes, transportit dhe institucioneve financiare.

Megjithatë, liderët duhet të bëjnë më shumë për të punuar me partnerët ndërkombëtarë dhe sektorin privat për të ndërtuar dhe zgjeruar kapacitetet përderisa Kosova kalon nga dixhitalizimi i operacioneve në sigurinë kibernetike. Masat e qëndrueshmërisë janë të nevojshme për të mundësuar që sektorët dhe institucionet të infrastrukturës kritike të rikuperohen, tejkalojnë dhe përshtaten me ndërprerjet nga sulmet kibernetike, dëmtimet fizike dhe ndryshimet klimatike. Partnerët ndërkombëtarë ofrojnë udhëzime mbi konceptet e qëndrueshmërisë. Komisioni Evropian e përkufizon qëndrueshmërinë e infrastrukturës kritike si sigurimin e stabilitetit dhe funksionimit të rregullt të jetës së përditshme sociale dhe ekonomike. Kjo zë zbatim në Kosovë përmes përafrimit me direktivat e Bashkimit Evropian dhe subjektet qeverisëse.

USAID-i i përfshin iniciativat e orientuara drejt detyrave nëpërmjet Critical Infrastructure Resilience Activities (Aktiviteteve të Qëndrueshmërisë së Infrastrukturës Kritike) (CIRA). USAID Kosova përshtat parimet e CIRA-s për zhvillimin e aktiviteteve dhe detyrave të fuqishme në njëmbëdhjetë sektorët të infrastrukturës kritike së Kosovës. CIRA është një investim i rëndësishëm në zhvillimin ekonomik, zhvillimin kombëtar dhe qytetarëve të Kosovës. Detyrat specifike përfshijnë forcimin e kornizave të qeverisjes së Kosovës dhe ndërtimin e kapaciteteve përmes, si për shembull, zhvillimit të fuqisë punëtore-ekspertëve kibernetikë, trajnimit të personelit për kërcënimet kibernetike, teknologjive inteligjente dhe CERT-it. Aktivitete të tjera përfshijnë të dhënat e inteligjencën lidhur me kërcënimet, vlerësimet e cenueshmërisë dhe zbutjen e rrezikut. Shkëmbimi i informacionit është një komponent tjetër kritik pasi promovon komunikimin ndërinstitucional dhe bashkëpunimin me sektorin privat për reagimin ndaj incidenteve dhe praktikat më të mira.

Efektiviteti i CIRA-s ndikohet nga planet e planifikimit, zhvillimit dhe zbatimit për të përmirësuar dhe ruajtur infrastrukturën kritike dhe për të rritur qëndrueshmërinë e publikut kundrejt rreziqeve të lidhura me klimën. Rreziqet klimatike rrisin nevojën për të promovuar sistemet e paralajmërimit të hershëm për thatësira, përmbytjet dhe nxehtësinë ekstreme, duke i lejuar operatorët të infrastrukturës kritike të marrin vendime proaktive dhe të zvogëlojnë prishjet për qytetarët dhe biznesin në Kosovë.

QEVERISJA E SIGURISË KIBERNETIKE TË KOSOVËS

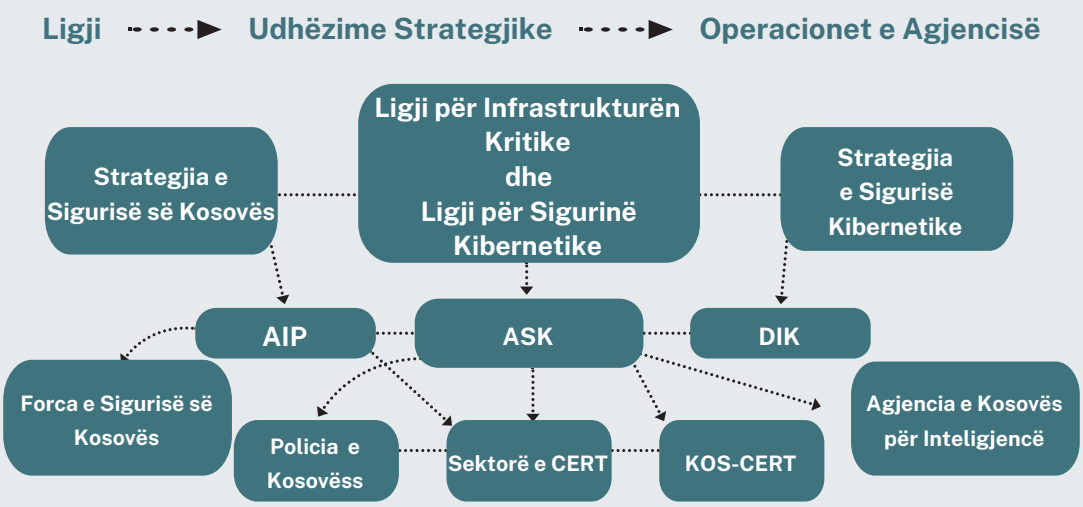
Qeveria e Kosovës po punon për të zhvilluar një kornizë koherente legjislative për të adresuar mospërputhjet ndërmjet kornizave aktuale ligjore dhe implementimit të agjencive të reja të krijuara me përgjegjësi për sigurinë kibernetike dhe mbrojtjen e infrastrukturës kritike. Kjo do të thotë që Qeveria e Kosovës duhet të harmonizojë me këmbëngulje legjislacionin me dokumentet kryesore që përcaktojnë prioritetet strategjike për mbrojtjen e hapësirës kibernetike të Kosovës dhe sektorëve të infrastrukturës kritike. Legjislacioni dhe prioritetet strategjike janë hartuar për të udhëhequr operacionet e agjencisë dhe koordinimin e institucioneve publike ekzistuese dhe atyre në zhvillim.

Ligjet dhe Kornizat Ligjore

Kosova miratoi Ligjin për Sigurinë Kibernetike (LSK) dhe themeloi Agjencinë e Sigurisë Kibernetike (ASK). LSK-ja ofron kornizën ligjore për formulimin e politikave dhe menaxhimit të sigurisë kibernetike, rregullimin e agjencive të sigurisë kibernetike dhe luftimin e aktiviteteve kriminale kibernetike. Derisa KOS-CERT së bashku me ekipet e tjera kombëtare si CERT-KP-RKS, CERT-KSF-RKS, ICT Academy CERT, dhe UBT-CERT janë përgjegjës për gjurmimin dhe reagimin ndaj incidenteve, dhe sapo ASK-ja të jetë plotësisht funksionale do të punojë me CERT për të ofruar përgjigje ndaj incidentit 24 orë/7 ditë dhe hapësirë të sigurt kibernetike.

Ashtu si LSK-ja, dhe Ligji për Infrastrukturën Kritike (LIK) **mbikëqyr 11 sektorët e sigurisë në Kosovë. E sektorët përfshijnë shëndetin publik, energjetikën, furnizimin me ujë, bujqësinë, TIK-un, shëndetin publik, shërbimet financiare, institucionet qeveritare, vlerat kombëtare, transportin dhe mallrat kombëtare. Ligji e përkufizon infrastrukturën kritike si një varg "sistemesh dhe asetesh qofshin ato fizike apo virtuale " specifike të sektorit, duke i dhënë prioritet zbutjes së rrezikut** dhe përmirësimit të sigurisë kombëtare dhe mirëqenies sociale. Por një qeverisje e fortë dhe efektive do të thotë përafrim i LSK-së dhe LIK-ut me Strategjinë e Sigurisë së Kosovës 2022-2027, Strategjinë e Sigurisë Kibernetike, dhe aktiviteteve për qëndrueshmërinë e infrastrukturës kritike.

Nevojitet një qasje praktike ndaj qeverisjes për të siguruar që institucionet publike të bashkëpunojnë me njëra-tjetrën dhe të bashkëpunojnë me sektorin privat. Ai gjithashtu duhet të sigurojë që qeverisja, kapacitetet dhe operacionet e agjencive janë në linjë. Legjislacioni dhe udhëzimet strategjike duhet të informojnë Agjencitë e Qeverisë së Kosovës, veçanërisht Agjencinë e Sigurisë Kibernetike, KOS-CERT dhe sektorët specifik të CERT-it, Agjencinë



për Informim dhe Privatësi, Divizionin e Infrastrukturës Kritike, Policinë e Kosovës, Forcëna e Sigurisë së Kosovës (FSK) dhe Agjencinë e Inteligjencës së Kosovës.

Strategjitë kryesore të sigurisë kibernetike

Strategjia e Sigurisë së Kosovës (SSK) 2002-2027 ofron udhëzime të përgjithshme në qeverisjen e sigurisë kibernetike dhe kapaciteteve kibernetike, inovacionit dhe teknologjisë, si dhe mbrojtjen e infrastrukturës kritike. SSK-ja i vendos katër fusha të fokusit strategjik duke përfshirë mbrojtjen e sovranitetit kombëtar dhe integritetit territorial, sigurimin e rendit kushtetues dhe sigurisë publike, promovimin e sigurisë njerëzore dhe zhvillimit njerëzor, integrimin brenda institucioneve dhe normave euroatlantike. Dizajni i SSK është modeluar sipas Strategjisë së Integruar të Shtetit të Departamentit të Shtetit të SHBA-ve.

Siguria kibernetike dhe infrastruktura kritike bien nën dispozitat e SSK për mbrojtjen e sovranitetit kombëtar dhe integritetit territorial dhe sigurinë energjetike dhe transformimin dixhital në kuadër të sigurisë njerëzore dhe zhvillimit social. Prandaj, udhëheqësit e Kosovës duhet të sigurojnë që veprimet pasuese të jenë të bazuara në udhëzimet e SSK-së. Sulmet kibernetike, shkeljet e të dhënave dhe fushatat e dezinformimit janë rrezik për sigurinë kombëtare të Kosovës po aq sa edhe armët konvencionale. Qeveria e Kosovës duhet të mbetet e përkushtuar për të përmirësuar aftësitë e mbrojtjes kibernetike, infrastrukturën e reagimit ndaj incidenteve dhe rritjen e ndërgjegjësimit për kërcënimet kibernetike. Pasi që SSK i pranon sfidat e Kosovës në hapësirën kibernetike, nevojiten kapacitete më të mëdha për t'u rikuperuar dhe për t'iu përgjigjur kërcënimeve kibernetike dhe fizike, rreziqeve dhe dobësive.

SSK-ja ia lë detajet e qeverisjes së sigurisë kibernetike Strategjisë së Sigurisë Kibernetike. Ky dokument drejton operacionet kibernetike dhe rrit qëndrueshmërinë dhe mbrojtjen kibernetike në 11 sektorët të infrastrukturës kritike së Kosovës. Ai vendos kornizat që angazhojnë Qeverinë e Kosovës të forcohet përmes investimeve në mbrojtjen kibernetike,

inovacionin, teknologjitë dhe prokurimet, zhvillimin e personelit dhe ndërtimin e kapaciteteve të sigurisë kibernetike nëpër institucionet publike.

Zyra e Kryeministrit për Qeverisje të Mirë krijoi Strategjinë e Sigurisë Kibernetike në vitin 2022 me mbështetjen e ofruar nga Modeli i Pjekurisë së Kapacitetit të Sigurisë Kibernetike për Shtetet- (Cybersecurity Capacity Maturity Model for Nations (CMM) përmes Qendrës Globale të Kapaciteteve të Sigurisë Kibernetike (GCSCC) - Global Cyber Security Capacity Centre (GCSCC). Strategjia është të forcojë mbrojtjen kibernetike dhe infrastrukturën kritike përmes bashkëpunimit publiko-privat, zhvillimit institucional, kornizave ligjore, ngritjes së kapaciteteve, reagimit ndaj incidenteve dhe bashkëpunimit me partnerët ndërkombëtarë, institucionet dhe organizatat joqeveritare.

Përpjekjet ekzistuese për sigurinë kibernetike janë nën përgjegjësinë e autoriteteve të zbatimit të ligjit. Krimet kibernetike dhe vjedhja e identitetit janë çështje për autoritet e zbatimit të ligjit, por sulmet kibernetike janë operacione keqdashëse të dizajnuara për të dëmtuar të gjithë sektorët të infrastrukturës kritike, duke kërcënuar kështu sigurinë kombëtare dhe ekonominë e Kosovës. Udhëzime më të qarta nevojiten për të përmirësuar koordinimin dhe udhëheqjen e ASK-së për mbrojtjen kibernetike të Kosovës dhe masave të infrastrukturës kritike.

Institucionet relevante për sigurinë kibernetike dhe mbrojtjen e infrastrukturës kritike

Agjencia e Sigurisë Kibernetike (ASK) është themeluar si agjenci udhëheqëse në reagim ndaj sulmeve kibernetike në rritje kundër Kosovës. Agjencia do të ketë përgjegjësi për mbrojtjen e hapësirës kibernetike të Kosovës, zbatimin e masave të mbrojtjes kibernetike, mbështetjen e KOS-CERT dhe reagimin ndaj incidenteve, dhe sigurimin e sistemeve të informacionit. Megjithatë, ASK aktualisht është në themelim e sipër dhe jo plotësisht funksionale.

Pasi të bëhet funksionale, ASK do të luajë një rol vendimtar në mbrojtjen e infrastrukturës digjitale dhe hapësirës kibernetike të Kosovës. Me njohjen e përgjithshme të mbrojtjes kibernetike në Strategjinë e Sigurisë së Kosovës dhe sigurinë kibernetike të paraqitur në Strategjinë e Sigurisë Kibernetike, ASK pritet të shërbejë si një organizatë e sigurisë kombëtare që i nënshtrohet më të mira, udhëzimeve etike dhe pajtueshmërisë. ASK duhet të sigurojë që vetëm profesionistë të trajnuar me njohuri, aftësi dhe përvojë në sigurinë kibernetike dhe të përkushtuar ndaj misionit do të punësohen për këto vende të punës. Proceset e vendimmarrjes së ASK-së duhet të jenë në konsultim me kolegët dhe palët e interesuara në agjencitë dhe ministritë e tjera të informuara nga industria private, akademia dhe grupet e shoqërisë civile.

Një fushë që ka nevojë për përkufizim dhe përsosje më të madhe është mbrojtja e shërbimeve të e-qeverisjes siç është platforma e-Kosova Tashmë, e-qeverisja monitorohet dhe mbikëqyret nga Agjencia e Shoqërisë së Informacionit (ASHI), e cila së bashku me ASK-në organizohet në kuadër të Ministrisë së Punëve të Brendshme. ASHI gjithashtu mbikëqyr zbatimin e TIK në institucionet publike. Tjetra është mënyra se si ASK do të ndërlidhet me Autoritetin Rregullativ të Komunikimeve Elektronike dhe Postare (ARKEP), i cili monitoron komunikimet elektronike dhe objektet postare duke përdorur shërbimet e e-qeverisjes.

Posa ASK të jetë plotësisht operacional, duhet të këshillojë dhe të ofrojë vlerësime të sigurisë për shërbimet e e-qeverisjes dhe sektorë të tjerë kritikë. ASHI dhe ARKEP ende mund të integrojnë çështjet e sigurisë kibernetike në rregulloret dhe standardet e tyre teknike. Agjencisë për Informim dhe Privatësi (AIP) të Kosovës i është besuar mbrojtja e privatësisë së të dhënave dhe adresimi i rrjedhjeve të të dhënave dhe zbatimi i masave të pajtueshmërisë etike dhe ligjore brenda udhëzimeve ligjore dhe rregullatore. AIP gjithashtu mbron qasjen publike në informacion dhe siguron llogaridhënie në qeverisje. Zyrtarët për Mbrojtjen e të Dhënave (ZMDh) i zbatojnë këto dispozita në institucionet publike.

AIP heton ankesat publike kundër agjencive qeveritare nëse të dhënat personale dhe privatësia shkelen, ndëshkon shkelësit dhe siguron zbatueshmërinë. AIP madje mbikëqyr portalet online që ofrojnë qasje në informacione dhe dokumente publike dhe promovon ndërgjegjësimin dhe edukon publikun dhe biznesin rreth privatësisë dhe mbrojtjes së të dhënave. AIP gjithashtu promovon ndërgjegjësimin publik kibernetik në mënyrë që njerëzit dhe bizneset të marrin vendime më të mira për mbrojtjen e të dhënave të tyre duke përdorur gjithashtu AIP-in si një resurs. Qeverisja duhet të sigurojë që zëri i AIP të dëgjohet në Agjencinë e Sigurisë Kibernetike. Që ai të mbetet efektiv, AIP ka nevojë për ZMDh më të trajnuar për të mbështetur dhe zgjeruar rolin e tij në mbrojtjen e institucioneve publike nga rrjedhjet e të dhënave, shkeljet dhe cenimet e privatësisë. Çelësi për këtë është sigurimi i punësimit dhe mbajtjes së talenteve më të mirë dhe më të kualifikuar, si dhe trajnimi i rregullt dhe i vazhdueshëm mbi praktikat më të mira të mbrojtjes së të dhënave.

Megjithatë, operacionet e agjencisë duhet të jenë efektive. Strukturat e Ministrisë së Punëve të Brendshme, aktet nënligjore në zhvillim dhe kornizat rregullatore duhet të harmonizohen për të shmangur konkurrencën dhe silotimin ndërmjet agjencive kibernetike të Qeverisë së Kosovës. Nevojitet një përkufizim dhe specifikë më e madhe në përcaktimin e roleve dhe përgjegjësive të ASK-së në mbrojtjen e infrastrukturës kritike në raport me Divizionin për Infrastrukturën Kritike (DIK). DIK mbron 11 sektorët e infrastrukturës së Kosovës, zhvillon zbutjen e rrezikut dhe koordinon protokollet e sigurisë në përputhje me mandatet në Ligjin për Infrastrukturën Kritike (LIK). Ndërtimi i lidhjeve midis mbrojtjes kibernetike dhe infrastrukturës kritike përmes kornizave të qeverisjes dhe bashkëpunimit ndërinstitucional është e rëndësisë parësore.

Në të kaluarën, mbështetja për operacionet e DIK-ut ka munguar. Që nga viti 2022, DIK përbëhej nga vetëm gjashtë anëtarë të stafit duke përfshirë drejtorin me përgjegjësi për 11 sektorët të infrastrukturës kritike të Kosovës. Vetëm gjashtë individëve iu besua përgjegjësia për telekomunikacionin, energjinë dhe spitalet në mesin e sektorëve të tjerë. DIK gjithashtu është penguar nga sfidat që lidhen me kapacitetet për ndërtimin e sektorëve të infrastrukturës kritike operative. DIK dhe ASK duhet të bashkëpunojnë dhe të koordinohen me njëri-tjetrin dhe të bashkëpunojnë me sektorin privat dhe partnerët nga SHBA-ja dhe BE-ja.

Qeverisja e centralizuar

Ndonëse nuk është plotësisht funksionale, AKS është pozicionuar si qendër nervore për rregullat, menaxhimin dhe rregulloret e politikave të sigurisë kibernetike, si dhe koordinimin ndërinstitucional dhe i mban agjencitë kibernetike përgjegjëse ndaj Strategjisë së Sigurisë së Kosovës dhe Strategjisë së Sigurisë Kibernetike. ASK është krijuar gjithashtu për të koordinuar dhe monitoruar aktivitetet dhe operacionet e infrastrukturës kritike dhe agjencive kibernetike, për të menaxhuar dhe mbikëqyrur reagimin ndaj incidenteve me KOS-CERT dhe CERT-të specifike të sektorit, si dhe shkëmbimin e të dhënave të inteligjencës dhe informacionit. ASK do të jetë përgjegjës për respektimin e vizionit strategjik të sigurisë kibernetike, identifikimin e rreziqeve dhe dobësive, dhe zhvillimin e vlerësimeve të inteligjencës së kërcënimeve të modeleve dhe trendeve në mjedisin më të gjerë. Agjencia e Inteligjencës së Kosovës dhe Forca e Sigurisë së Kosovës duhet të jenë pjesë e këtij procesi duke pasur parasysh asetet që ato sjellin në drejtimin strategjik dhe kapacitetet operacionale.

Proceset e vendimmarrjes kibernetike duhet të zhvillohen përmes ASK dhe KOS-CERT për të siguruar që reagimi ndaj incidentit, zbutja e rrezikut, analiza e cenueshmërisë dhe zhvillimi i fuqisë punëtore, të lidhen me njëra tjetrën. Një sistem vendimmarrës i centralizuar me një ASK me burime që drejton dhe koordinon procesin do të rrisë qëndrueshmërinë dhe do të forcojë pozitën e Kosovës në luftimin e krimit kibernetik, hakimeve dhe incidenteve kibernetike në infrastrukturën kritike dhe shkeljet e të të dhënave.

Arritja te Qëndrueshmëria

Arritja në qëndrueshmëri do të thotë që kornizat qeverisëse të Kosovës duhet t'i japin prioritet kapitalit njerëzor. Zhvillimi i kompetencës dhe ekspertizës si në sektorin publik ashtu edhe në atë privat në nivelet strategjike, operacionale dhe teknike janë të substanciale për qëndrueshmërinë. Qeverisja ka të bëjë me sigurimin që kapacitetet janë në përputhje me sundimin e ligjit dhe udhëzimet strategjike. Por qeverisja në mungesë të një angazhimi të përkushtuar ndaj kapaciteteve nuk është qeverisje.

Agjencitë e Kosovës për sigurinë kibernetike dhe infrastrukturën kritike duhet të kenë burime për të përmbushur misionet e tyre për të përmbushur misionet e tyre dhe për të arritur objektivat sipas udhëzimeve etike dhe praktikave më të mira. Ata duhet të kenë autoritetin për t'iu përgjigjur incidenteve kibernetike, si dhe autorizime për t'i vlerësuar ato, për të mbledhur dhe analizuar të dhënat e inteligjencës dhe informacionin, për të mbrojtur të drejtat dhe të dhënat e privatësisë dhe për të bashkëpunuar me autoritetet e zbatimit të ligjit, bizneset dhe partnerët ndërkombëtarë. Vetëm një ekspertë kibernetikë kompetent, i trajnuar mirë dhe e paguar mirë mund t'i kryejë këto detyra.

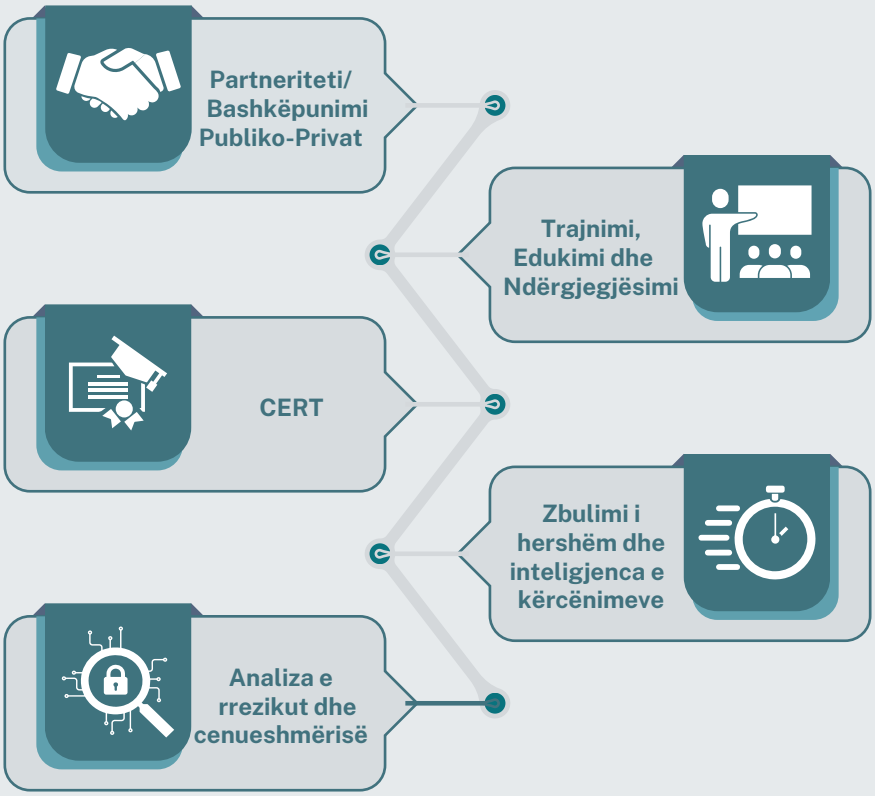
Nëse Kosova dëshiron të rimëkëmbet në mënyrë efektive dhe të zmbrapsë sulmet e ardhshme nga aktorët keqdashës dhe ndryshimet klimatike, atëherë ajo duhet të lidhë qeverisjen me kapacitetet. Korniza qeverisëse e Kosovës duhet të ketë prioritet ndërtimin e një fuqie punëtore të sigurisë kibernetike dhe një mentalitet të sigurisë kibernetike.

NDËRTIM KAPACITETEVE

Ndërtimi i kapaciteteve është thelbësor për mbrojtjen kibernetike të Kosovës dhe qëndrueshmërinë e infrastrukturës kritike. DIK dhe AIP, dhe së shpejti me ASK-në, do të luajnë role kyçe në mbrojtjen e hapësirave dixhitale të Kosovës, zbutjen e rreziqeve dhe dobësive, forcimin e të dhënave të inteligjencës lidhur me kërcënimet dhe përdorimin e teknologjive me përgjegjësi. Të përfshira në këto masa janë edukimi dhe ndërgjegjësimi për sigurinë kibernetike, KOS-CERT, dhe të dhënat inteligjente lidhur me kërcënimet me ASK-në dhe partneritetin publik-privat në qendër të të treve.

Një fuqi punëtore e trajnuar që përdor teknologjinë me përgjegjësi luan gjithashtu një rol kyç në ndërtimin e infrastrukturës kritike dhe qëndrueshmërisë ndaj klimës. Ndonëse teknologjitë dhe mjetet janë lehtësisht të disponueshme për t'u përdorur në zbulimin e hershëm dhe inteligjencën e kërcënimeve, personeli në institucionet publike duhet gjithashtu të angazhohet në zhvillimin profesional për të ecur në hap me praktikat më të mira. Njerëzit duhet të jenë të përditësuar rregullisht.

ZONAT E NGRITJES SË KAPACITETEVE



Arsimimi i Lartë, Trajnimet dhe Ndërgjegjësimi i Publikut

ASK dhe agjencitë e tjera janë qenësore në promovimin e ndërgjegjësimit të publikut për sigurinë kibernetike dhe qëndrueshmërinë të infrastrukturës kritike. Fushatat e edukimit dhe informimit, konferencat dhe punëtoritë, angazhimi me universitetet dhe shkollat, dhe bashkëpunimi me grupet e shoqërisë civile janë jashtëzakonisht të rëndësishme në ndërtimin e sigurisë kibernetike dhe qëndrueshmërisë.

Ka mekanizma edukativë që funksionojnë në Kosovë për shumë vite që shërbejnë si burime të njohurive dhe kërkimeve për sigurinë kibernetike. Këtu përfshihen institucionet publike dhe private të arsimit të lartë dhe sektorët e konsulencës joqeveritare e private. Edhe pse ka disa universitete dhe kolegje në Kosovë që ofrojnë diploma për sigurinë kibernetike dhe TIK-un, duhet bërë më shumë punë për të siguruar që lidhjet dhe kanalet të krijohen dhe mirëmbahen në mes të Agjencive të Qeverisë së Kosovës për sigurinë kibernetike dhe të infrastrukturës kritike, institucioneve të arsimit të lartë dhe programeve të trajnimit.

Instituti i Teknologjisë Rochester-Kosovë ofron diplomë të nivelit Bachelor of Science në informatikë dhe teknologji informacioni dhe kurse trajnimi për TIK dhe zhvillim profesional, dhe ofron projekte për Sigurinë Kibernetike dhe Internet of Things. Gjithashtu, Kolegji AAB ofron diploma universitare në sigurinë kibernetike dhe programim diplomë Master of Science të programit në shkenca kompjuterike. Ai gjithashtu menaxhon Laboratorin e Qendrës së Sigurisë Kibernetike i cili fokusohet në sigurinë e të dhënave në internet.

Universiteti i Biznesit dhe Teknologjisë (UBT) ofron programe dhe qendra të sigurisë kibernetike dhe TIK me fokus në Sigurinë Kibernetike dhe Privatësinë, Zhvillimin dhe Inovacionin e Softuerit, Modelimin dhe Simulimin si dhe Statistikat, Përpunimin e të Dhënave dhe Parashikimin. UBT gjithashtu mirëmban Sistemin e Raportimit të Incidentit UBT-CERT që merr raporte mbi shkeljet dhe cenueshmëritë kibernetike dhe të të dhënave. Universiteti i Prishtinës ofron projekte të edukimit kibernetik në kursin Cyber Hygiene e-Learning, projekte bashkëpunuese duke përdorur teknologjitë e Internet of Things dhe hulumtimin dhe inovacionin. Universiteti i Gjilanit ofron një program universitar në shkenca kompjuterike dhe një program pasuniversitar në sistemet e kontrollit dhe inteligjencës artificiale dhe një tjetër në e-qeverisje.

Institucionet akademike në Kosovë ofrojnë programim arsimor të TIK-ut dhe kanë sinergji me komunitetin e biznesit. Por përderisa ka një sektor privat dinamik të TI-së në Kosovë, ka pak theks në partneritetet e sigurisë kibernetike me agjencitë e sigurisë kibernetike të Qeverisë së Kosovës dhe të infrastrukturës kritike. Qeveria e Kosovës publikoi një dokument në vitin 2023 që specifikonte nenet për krijimin e Qendrës Shtetërore të Trajnimit të Sigurisë Kibernetike të Kosovës e që duhej të përmbushte qëllimet e ndërtimit të një kulture të sigurisë kibernetike dhe zhvillimin e programeve të trajnimit. Misioni dhe nenet e vendosin QSHTSK-në në kuadër të Ministrisë së Mbrojtjes dhe Forcës së Sigurisë së Kosovës. Dokumenti e përmend krijimin e Cyber Range(Poligonin Kiberenetik) për të modeluar dhe simuluar modelet dhe vektorët e sulmeve kibernetike.

Përveç publikimit të neneve, QSHTSK-ja ende nuk është funksionale. Informacioni i dhënë

tregon se QSHTSK-ja nuk do të filloj punën e saj si qendër trajnimi më së largu deri në muajin mars të vitit 2024. Ligji për sigurinë kibernetike riaktualizon qendrat e trajnimit për sigurinë kibernetike. Megjithatë, disa hapa konkretë janë ndërmarrë, gjë që mund të nënkuptojë se Agjencia e Sigurisë Kibernetike do të luajë një rol më të madh në programet e trajnimit të mbështetura nga shteti.

Qendrat e trajnimit për sigurinë kibernetike ekzistojnë në Kosovë, por në sektorin privat. Cyber Academy (Akademia Kiberentike) ofron një kurrikulë plotësisht të zhvilluar për trajnimin e sigurisë kibernetike, si dhe mundësitë e zhvillimit profesional për kompanitë që kërkojnë të përmirësojnë aftësitë kibernetike të punonjësve të tyres. Gjithashtu, CISTCK është një kompani softuerësh dhe konsulence që është e specializuar në pen-testime, analizën e cenueshmërisë, të dhënat e inteligjencës rreth kërcënimeve dhe zbulimin e hershëm, dhe auditimet e kontrollit të sigurisë. Për më tepër, National Institutes of Standards and Technology (NIST) u ofron klientëve programe trajnimi në US National Institutes of Standards and Technology (NIST) Institutin Kombëtar të Standardeve dhe Teknologjisë të SHBA-së) dhe Open Worldwide Application Security Project (OWASP) (Projektin e Sigurisë së Aplikimeve të Hapura Botërore) në shkallë ndërmarrje për të siguruar aplikacione nga sulmet kibernetike. Përveç kësaj, Cactus Education është një OJQ dhe kompani konsulente që ofron dy programe profesionale studimi në administrimin e sistemit dhe rrjetit dhe zhvillimin e aplikacioneve në ueb faqe dhe telefona celular.

Në sektorin joqeveritar Innovation Centre Kosovo, e cila ofron kurse trajnimi kibernetike dhe konsultime biznesi, programet specifike përfshijnë Cyber Unity Academy(Akademinë e Unitetit Kibernetik) , Cyber Training (Trajnimin Kibernetik), International Cyber Security Exercise (Ushtrimin Ndërkombëtar të Sigurisë Kibernetike), One Step Ahead Cyber Security Education (Edukimin për Sigurinë Kibernetike Një Hap Përpara), Cyber Defense Week(Java e Mbrojtjes Kibernetike), dhe Crypton. Megjithatë, ka edhe hyrje të tjera në këtë fushë, përkatësisht Albanian Cyber Association (Shoqata Kibernetike Shqiptare), një OJQ që punon me grupet e shoqërisë civile për të rritur ndërgjegjësimin e publikut për sigurinë kibernetike dhe promovon konkurrencën dhe zhvillimin profesional.

Një fuqi punëtore kibernetike e trajnuar më mirë dhe me përvojë në institucionet publike do të përmirësojë reagimin dhe rikuperimin ndaj incidenteve. Por sektori publik qëndron prapa në këtë fushë dhe është përtej sektorit privat në ofrimin e programeve të trajnimit dhe rritjen e ndërgjegjësimit publik për përdorimin e sigurt të internetit. Masat për ngritjen e kapaciteteve duhet t'i japin përparësi këtyre përpjekjeve duke zhvilluar programe partneriteti me institucionet e arsimit të lartë dhe sektorin privat.

Agjencitë e sigurisë kibernetike dhe të infrastrukturës kritike duhet të zhvillojnë incentiva për karrierë për të tërhequr dhe mbajtur profesionistë të talentuar në institucionet publike për të zbutur ikjen e trurit. Shfrytëzoni programet e mësimit eksperimental me universitetet dhe kolegjet dhe OJQ-të dhe konsulencat për të ndërtuar një varg talentesh dhe ofroni pako solide kompensimi dhe përfitimesh që janë konkurruese me sektorin privat. Pastaj, ofroni zhvillim profesional në mënyrë që fuqia punëtore kibernetike të mund të qëndrojë e përditësuar mbi etikën, praktikat më të mira, operacionet dhe teknologjitë.

Kjo do të thotë se legjislacioni dhe kornizat rregullatore të sigurisë kibernetike të Qeverisë së Kosovës kanë nevojë për harmonizim më të madh me kompanitë kibernetike të sektorit privat dhe operatorët të infrastrukturës kritike. Ministria e Ekonomisë dhe Ministria e Arsimit të Kosovës kanë nevojë për resurse për të inkurajuar të rinjtë kosovarë që të qëndrojnë në vend dhe të sigurojnë pozita në kuadër të fuqisë punëtore kibernetike të sektorit publik. Rezultat i e kësaj është zhvillimi dhe ruajtja e normave që vlerësojnë institucionet publike dhe bizneset e sektorit privat në sigurinë kibernetike dhe qëndrueshmërinë të infrastrukturës kritike.

Partneritetet Publiko-Private

Për të përmbushur këto detyra dhe për t'i mbështetur ato me kalimin e kohës, institucionet publike dhe sektori privat duhet të jenë partnerë me njëri-tjetrin në frymën e bashkëpunimit. Ndërtimi i një kulture të partneriteteve publike-private do të ndihmojë sigurinë kibernetike dhe qëndrueshmërinë e infrastrukturës kritike në Kosovë. Institucionet publike luftojnë për të krijuar qëndrueshmëri kibernetike për shkak të mungesës së personelit të trajnuar për sigurinë kibernetike dhe infrastrukturës së vjetër të TIK-ut. Institucionet publike mund të mësojnë nga sektori privat dhe duhet të bashkëpunojnë me firmat dhe bizneset në shkëmbimin e informacionit, teknologjitë e sigurta, edukimin dhe ndërgjegjësimin kibernetik, si dhe zhvillimin dhe trajnimin profesional të personelit kibernetik. Bashkëpunimi publik-privat është një sfidë, por kërkon vëmendje nëse siguria kibernetike dhe qëndrueshmëria e infrastrukturës kritike do të vije në shprehje në Kosovë.

Sektori privat i Kosovës e ka shqetësimin për kujdesin lidhur me mbrojtjen e aseteve të tyre financiare, të dhënave të klientëve, privatësisë dhe pronës intelektuale. Megjithatë, kompanive më të vogla u mungojnë burimet për të zhvilluar masa të sigurisë kibernetike dhe për të përdorur teknologjitë për vlerësimin e kërcënimeve dhe reagimin ndaj incidenteve në krahasim me institucionet publike të cilave u është besuar mbrojtja e infrastrukturës kritike në nivel makro, sigurimi i të dhënave publike dhe privatësisë dhe siguria publike.

Burimet ekzistuese mund të lehtësojnë bashkëpunimin ndërmjet institucioneve publike të Kosovës dhe kompanive private. Innovation Centre Kosovo- Qendra e Inovacionit në Kosovë (ICK) ndihmon dhe mbështet firmat e sektorit privat me konsultime, trajnime dhe zgjidhje inovative. ICK ofron hapësirë për zyra, këshillim dhe programe edukative, punëtori dhe evente publike për startup-et dhe firmat në sektorë të ndryshëm. ICK ka një histori të fortë suksesi në lehtësimin e partneriteteve dhe programimit bashkëpunues.

Gjithashtu, Cyber Zero, i cili mbështetet nga Ambasada e SHBA-së në Prishtinë, ofron burime për palët e interesuara në agjenci dhe firma kibernetike që të angazhohen me njëri-tjetrin për praktikat më të mira, etikën dhe pajtueshmërinë, dhe kërcënimet kibernetike.

Zhvillimi i Kapaciteteve në Sektorët e Infrastrukturës Kritike

Operatorët e infrastrukturës kritike në energji, shërbimet e-qeverisjes dhe telekomunikacionit janë gjithnjë e më shumë të varur nga teknologjitë dixhitale të ndjeshme ndaj sulmeve kibernetike. Në sektorin energjetik të Kosovës, kërcënimet përbëhen nga sulmet e DoS (ndërprerja e shërbimeve) në rrjetet e energjisë, sulmet kibernetike mbi sistemet e kontrollit dhe manipulimi i të dhënave të energjisë. Dobësitë e Sektorit të energjisë përfshijnë resurse të kufizuara dhe kufizime buxhetore që parandalojnë zgjidhjet më moderne për sulme të sofistikuara dhe të synuara dhe mungesën e përvojës në sigurinë kibernetike.

Procedurat dhe proceset duhet të zbatojnë protokollet e sigurisë për Supervisory Control and Data Acquisition (SCADA)- (sistemet e kontrollit mbikëqyrës dhe të grumbullimit të të dhënave), duke kufizuar kështu nevojën për personel në terren. Kjo është e rëndësishme për menaxhimin e rrjetit të energjisë, impianteve të trajtimit të ujit, energjisë, transportit dhe telekomunikacionit Për menaxhimin e rrjetit të energjisë, sistemet SCADA monitorojnë tensionin dhe rrjedhën e energjisë, duke u mundësuar operatorëve të infrastrukturës kritike të sigurojnë operime të rregullta, të zbulojnë kërcënimet, të zbusin rreziqet dhe të parandalojnë defektet. Sistemet SCADA mundësojnë kontrollin në distancë të nënstacioneve dhe pajisjeve të tjera dhe rrisin efikasitetin. Ato ndihmojnë gjithashtu në kuptimin dhe monitorimin e kërkesës dhe shpërndarjes së energjisë. Në sistemet e ujit, sistemet SCADA u mundësojnë operatorëve të mbikëqyrin trajtimin e vazhdueshëm dhe të automatizuar të ujit për konsumim të pastër dhe të sigurt për qytetarët dhe të identifikojnë pompat dhe valvulat me defekt. SCADA efektive monitoron ndryshimet në rrjedhën e ujit dhe mbikëqyr rezervuarët dhe shpërndarjen.

Fusha të tjera kërkojnë implementim të mirë të sistemeve SCADA. Ky është veçanërisht te rasti për gjurmimin dhe sigurimin e shpërndarjes dhe transportit të sigurt dhe efikas të naftës dhe gazit natyror në Kosovë. Sistemet SCADA gjithashtu duhet të monitorojnë të dhënat mbi fluksin e trafikut, tollovitë dhe incidentet e veturave dhe të komunikojnë me organet e zbatimit të ligjit. Kjo do të lejojë automatizimin e detyrave dhe operacioneve, zbutjen e ndërprerjeve dhe incidenteve dhe promovimin e menaxhimit të besueshëm të infrastrukturës.

Në telekomunikacion, kërcënimet përfshijnë shkeljen e të dhënave, infiltrimin në rrjetet dixhitale dhe spiunazhin kibernetik, përgjimin në rrjetet e komunikimit dhe komutimin e SIM kartelave. Këto kërcënime mund të shfrytëzojnë sigurinë e pamjaftueshme të të dhënave, protokollet e dobëta të autentifikimit , softuerin e vjetërsuar dhe Internet of Things (IOT). Procedurat kibernetike fokusohen në enkriptimin e të dhënave, autentifikimit me shumë faktorë (MFA), përditësimin e rregullt të softuerit dhe përmirësimet e vazhdueshme në monitorimin e rrjetit. Megjithatë, mekanizmat institucionalë të Ministrisë së Punëve të Brendshme duhet të sigurojnë që këto procedura të realizohen plotësisht.

Shërbimet e e-qeverisjes sigurojnë në mënyrë efektive administrim publik të dixhitalizimit të shërbimeve elektronike. Qeveria e Kosovës ka prioritet zhvillimin e shërbimeve të e-qeverisjes përmes e-një strategjie për e-qeverisjen (2023-2027) që hyri në fuqi në vitin 2023. Strategjia është krijuar për të bërë ndërveprime dixhitale me shërbimet qeveritare miqësore për

përdoruesit, duke minimizuar gjithashtu frustrimin e qytetarëve, për të zbutur kostot publike dhe për të përmirësuar rritjen ekonomike kombëtare. Strategjia e e-qeverisjes përcakton vizionin e përgjithshëm për dixhitalizimin e avancuar të zbatimit të politikave publike dhe administratës publike dhe transparencës. Përvoja pozitive e përdoruesve me shërbimet e e-qeverisjes rrit besimin dhe besimin e publikut në qeverinë e Kosovës dhe ndërveprimet pozitive me shërbimet administrative përmirësojnë efektivitetin dhe llogaridhënien.

Qytetarët e Kosovës mund të kenë qasje dhe të përdorin platformën e-Kosova e cila shërben si një qendër për shërbimet publike elektronike. Shërbimet e e-Kosova, përfshijnë taksat, shëndetin publik, shërbimet sociale, regjistrimin e automjeteve, statusin e shtetësisë, rregulloret pronësore, shërbimet komunale, procedurat gjyqësore, avokatin e popullit, pensionet, grantet dhe subvencionet, arsimin, çështjet konsullore, auditimet ligjore, punën dhe punësimin, dhe verifikimi i dokumentit. Pasi përdoruesit të krijojnë llogari përmes mjeteve të verifikuara të regjistrimit në rubrikat e kërkuara, ata mund të kenë qasje në shërbime dhe programe. e-Kosova ka qenë e suksesshme në dixhitalizimin e shërbimeve publike që dikur ishin ekskluzivisht në cilësinë vetëm personale.

Megjithatë, rreziqet dhe dobësitë mbeten prezente. Më 5 shtator 2022, e-Kosova dhe shërbimet e tjera qeveritare ishin cak i një sulmi të shpërndarë të paralizimit të shërbimit që ndërpreu shërbimet, duke mbingarkuar funksionet e rregullta të e-qeverisjes. Ndonëse rreziku u zbut, nevojiten burime shtesë për CERT të trajnuar për të kuptuar modelet dhe tendencat e sulmeve kibernetike dhe për të bashkëpunuar me sektorin privat dhe partnerët ndërkombëtarë.

Zbulimi i hershëm dhe të dhënat inteligjente rreth kërcënimeve

Sistemet e zbulimit të ndërhyrjeve, firewalls, dhe mjetet e monitorimit, do të ndihmojnë në gjurmimin e kërcënimeve kibernetike dhe sigurimin e operacioneve të infrastrukturës kritike. Kontrollet e qasjes dhe kodimet zvogëlojnë efektet e rrezikshme të incidenteve kibernetike dhe përmirësojnë rikuperimin nga ndërprerjet dhe sulmet. Rritja e trajnimit të fuqisë punëtore kibernetike, zhvillimi profesional dhe kontakti me publikun plotësojnë këto masa. Sistemet e sigurta të komunikimit dhe shkëmbimit të informacionit do të promovojnë bashkëpunimin dhe partneritetet kur sektorët të infrastrukturës kritike janë objekt sulmi ose përjetojnë ndërprerje. Mjetet dhe programet analitike mund të ndihmojnë personelin e sigurisë të marrë vendime efektive të bazuara në të dhëna, të zhvillojë analiza të rrezikut dhe të bëjë investime dhe shpërndarje më optimale të burimeve.

Të dhënat Inteligjente kredibile dhe solide ndaj kërcënimeve shërben si një instrument vital në sigurinë kibernetike dhe infrastrukturën kritike të Kosovës pasi mund të ndihmojë reagimin ndaj incidentit përmes identifikimit dhe vlerësimit të kërcënimeve kibernetike dhe akterëve keqdashës. Të dhënat Inteligjente lidhur me kërcënimet është thelbësore në mbrojtjen kibernetike dhe infrastrukturën kritike, sepse ndihmon në zbulimin e hershëm përmes identifikimit dhe monitorimit të kërcënimeve të reja përpara se akterët keqdashës të shkaktojnë dëme. Inteligjenca lidhur me kërcënimit ndihmon me të kuptuarit e taktikave, teknikave dhe procedurave (TTP) të akterëve të kërcënimit dhe shkallën në të cilën kërcënimet

përputhen me modelet dhe tendencat me kalimin e kohës. Kjo do të informojë më mirë sektorët e buxheteve të agjencive duke ndihmuar në drejtimin e burimeve në fushat prioritare.

Të dhënat Inteligjente lidhur me kërcënimet gjithashtu ndihmojnë në mbrojtjen e infrastrukturës kritike, veçanërisht sektorët e energjisë, transportit dhe telekomunikacionit. Në energji, të dhënat Inteligjente lidhur me kërcënimet mund të zvogëlojë rrezikun për tubacionet, rrjetet e energjisë elektrike dhe termocentralet/nënstacionet duke vëzhguar tendencat në peizazhin e kërcënimit. Në transport, ai mund të minimizojë rreziqet për aeroportet dhe kontrollet e trafikut ajror dhe rrugëve. Në telekomunikacion, të dhënat inteligjente lidhur me kërcënimet mund të identifikojë modele në aktivitetin keqdashës në ofruesit e shërbimeve të internetit dhe rrjetet celulare përpara se të sulmojnë.

Strategjia e sigurisë kibernetike e Kosovës i jep përparësi zhvillimit të inteligjencës së besueshme dhe të aksesueshme lidhur me kërcënimet me koleksione të inteligjencës nga burimet hapura/publike dhe analiza të informacionit të disponueshëm publikisht. Një kulturë e Inteligjencës lidhur me kërcënimet dhe shkëmbimit të informacionit me institucionet publike, përkatësisht Agjencinë për Informacion dhe Privatësi, Divizionin për Infrastrukturën Kritike, Agjencinë e Inteligjencës së Kosovës dhe Forcën e Sigurisë së Kosovës dhe aktorët e jashtëm si Agjencia Amerikane e Sigurisë Kibernetike dhe Infrastrukturës (CISA), Agjencia për Sigurinë Kibernetike e BE-së si dhe personelin me certifikatë sigurie në firmat private të Inteligjencës lidhur me kërcënimet.

Softueri dhe aplikacione të tjera janë të disponueshme për abonim dhe duhet të blihen Për shembull, Alien Vault ofron raportime në kohë reale mbi kërcënimet, sulmet dhe dobësitë e reja duke përdorur burime të ndryshme publike. Kjo i lejon analistët e kërcënimeve të fitojnë njohuri dhe të vlerësojnë peizazhin e kërcënimit ndërsa ai evoluon dhe zhvillohet. Alien Vault's Open Threat Exchange (Shkëmbimi i Hapur i Kërcënimeve të Alien Vault) është një mjedis i hapur me ekspertë që ndajnë informacione mbi kërcënimet e reja.

Zbutja e rrezikut dhe vlerësimi i cenueshmërisë

Siguria kibernetike dhe mbrojtja e infrastrukturës kritike nënkupton kryerjen e kontrollës së rregullt të zbutjes së rrezikut dhe skanimit të cenueshmërisë. Infrastruktura dixhitale e Kosovës është veçanërisht e ndjeshme ndaj incidenteve kibernetike dhe sulmeve nga qeveritë, grupet përfaqësuese dhe kriminelët kibernetikë. Aktorët keqdashës shtetërorë dhe joshtetërorë shfrytëzojnë dobësitë, prishin shërbimet thelbësore, kryejnë spiunazh kibernetik, zbrazin llogaritë bankare dhe vjedhin informacione të pronarit. Ata gjithashtu kombinojnë sulme malware dhe ransomware me akte fizike terrorizmi, sabotazhi dhe dhunë të tjera.

ASK dhe DIK duhet të i përmbahen raportit të vlerësimit të rrezikut diagnostik të Bankës Botërore për të zbutur kërcënimet dhe dobësitë në sistemet kritike. Punësimi, trajnimi, promovimi dhe mbështetja e personelit përmes programeve dhe iniciativave të zhvillimit profesional mbështesin vlerësimin e rrezikut, zbutjen e kërcënimeve dhe reagimin ndaj incidenteve. Vlerësimi i cenueshmërisë dhe skanimi dhe analizat e rrezikut janë për qëllime të qëndrueshmërisë dhe zbatimit të masave mbrojtëse. Rritja e qasjes në teknologji do të luajë

një rol vital në krijimin e qëndrueshmërisë të infrastrukturës kritike në Kosovë, pasi që vendi përballet me kërcënimet kibernetike, sulmet kibernetike dhe ndryshimet klimatike. Kryerja e skanimit të rregullt dhe të vazhdueshëm të cenueshmërisë duke përdorur aplikacione softuerike ndihmon në zbulimin e cenueshmërisë në sektorët kryesorë.

Institucionet publike kanë nevojë për akses në mjete dhe aplikacione softuerike për të asistuar në skanimin e dobësive tyre dhe përpjekjet për zbutjen e rrezikut. Për shembull Nessus vulnerability scanner (skaneri i cenueshmërisë Nessus), përdoret në sigurinë e rrjetit për të vlerësuar portat e kompjuterit, operacionet e rrjetit dhe ekzaminimin për dobësitë e brendshme që mund të shfrytëzohen nga akterët që kërkojnë të ndërpresin ose çaktivizojnë sistemet kritike. Menaxhimi i cenueshmërisë . Qualys identifikon dhe rregullon dobësitë në IT, teknologjinë operacionale dhe Internet of Things.

Zeek është një mjet me burim të hapur që monitoron trafikun e rrjetit dhe zhvillon regjistrat e transaksioneve dhe përmbajtjen e skedarëve për analizën dhe rishikimin e rrjetit. Infrastruktura dhe mjetet e automatizimit siç janë Splunk dhe LogRhythm grumbullojnë dhe analizojnë regjistrat nga burimet publike për të zbuluar incidentet në kohë reale. Ndoshta më me ndikim do të jetë futja e praktikave të autentifikimit me shumë faktorë (MFA) (MFA) në mbarë Kosovën. MFA do të parandalojë rrjedhjet e të dhënave dhe aksesin e paautorizuar në informacionin e klasifikuar ose të pronarit. CyberArk dhe Okta janë platforma që mund të ndihmojnë në monitorimin e lejeve në sistemet kritike. Për më tepër, mjetet e kodimit të të dhënave mund të mbrojnë nga aksesi i paautorizuar dhe shërbimet cloud Microsoft Azure dhe AWS Security mbrojnë të dhënat në një arkitekturë të sigurt cloud.

Përdorimi i përgjegjshëm dhe etik i këtyre mjeteve është thelbësor pasi analistët duhet të kenë personel me certifikatë të sigurisë e të cilët i respektojnë normat, ligjet dhe rregulloret. Përdoruesit duhet të pajisen me autorizim përpara se të përdorin skanerët e cenueshmërisë, analizën e rrjetit dhe koleksionet dhe analizat e të dhënave të inteligjencës lidhur me kërcënimet. Trajnimi i rregullt dhe zhvillimi profesional i personelit në përdorimin e përgjegjshëm të teknologjive dhe praktikave më të mira të sigurisë kibernetike janë thelbësore. Përdorimi i teknologjisë në mungesë të praktikave më të mira, trajnimit të duhur dhe standardeve të pajtueshmërisë nuk është etike.

REKOMANDIMET

1. Të Centralizohen dhe koordinohen operacionet kibernetike dhe të infrastrukturës kritike. AIP dhe DIK kanë nevojë për integrim më të mirë në proceset vendimmarrëse të sigurisë në Kosovë dhe një marrëdhënie të fortë pune me Agjencinë e Sigurisë Kibernetike. ASK duhet të jetë në qendër të këtij procesi.

2. Përafroni dhe fuqizoni operacionet e ASK-së, DIK-ut dhe AIP-së në kuadër të Strategjisë së Sigurisë së Kosovës dhe Strategjisë së Sigurisë Kibernetike me kompetenca nga legjislacioni dhe kornizat ligjore. Lidhni qeverisjen me njohuritë duke siguruar që Strategjia e Sigurisë së Kosovës dhe Strategjia Kombëtare e Sigurisë Kibernetike të rezultojnë në veprime të zbatueshme.

3. Zhvilloni programe trajnimi dhe zhvillimi profesional të gjithë qeverisë mbi parimet e sigurisë kibernetike dhe reagimin ndaj incidenteve. Ndërtoni një siguri kibernetike të trajnuar, kompetente dhe të edukuar në Kosovë me programe trajnimi të mbështetura nga shteti të koordinuara nga ASK-ja dhe partnerë nga ndërmarrjet e sektorit privat dhe OJQ-të për të maksimizuar njohuritë.

4. Zhvilloni kapacitetet sociale/njerëzore përmes një përpjekjeje të gjithë shoqërisë për të promovuar ndërgjegjësimin e publikut për rreziqet e kërcënimeve kibernetike dhe nevojën për të raportuar aktivitete të dyshimta.

5. Pasqyroni hartën e sektorëve të infrastrukturës kritike përmes një vlerësimi të bazuar në nevojat për energjinë, transportin, trajtimin e ujit, telekomunikacionin dhe e-qeverisjen.

6. Mbështetni dhe praktikoni analizën e rregullt të cenueshmërisë dhe vlerësimin e rrezikut duke investuar në aplikacione dhe mjete softuerike të sigurta dhe trajnime për përdorim etik dhe të përgjegjshëm.

7. Bashkëpunoni me partnerë ndërkombëtarë dhe kërkoni ndihmë teknike nga sektori privat për të ndarë njohuritë e sigurisë kibernetike, të dhënat e inteligjencën lidhur me kërcënimet dhe praktikat më të mira.

Katalogimi në botim – (CIP)

Biblioteka Kombëtare e Kosovës “Pjetër Bogdani”

355.02(496.51)(047)

Dolan, Chris J.

Rruga drejt qëndrueshmërisë : qeverisja dhe ndërtimi i kapaciteteve në Sigurinë Kibernetike dhe Infrastrukturën Kritike të Kosovës / Chris J. Dolan. -Prishtinë : QKSS, 2024. -16 f. : ilustr. ; 26 cm.

ISBN 978-9951-842-19-8

QKSS
Qendra Kosovare për Studime të Sigurisë

Rreth QKSS

E themeluar në prill të vitit 2008, Qendra Kosovare për Studime të Sigurisë (QKSS) është një organizatë e specializuar dhe e pavarur 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 tepër detaje rreth QKSS, mund të referoheni tek:

www.qkss.org
www.securitybarometer.qkss.org

@KCSSQKSS

ISBN 978-9951-842-19-8