REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

RAPORT

QEVERISJA E SIGURISË KIBERNETIKE NË SHQIPËRI

VITI 2023

I. HYRJE

Ky raport përshkruan situatën e qeverisjes së sigurisë kibernetike në Republikën e Shqipërisë gjatë vitit 2023. Për të paraqitur situatën e qeverisjes së sigurisë kibernetike është me rëndësi të kuptohet kompleksiteti dhe konteksti i zhvillimit të kësaj fushe si dhe rëndësia e saj për shoqërinë dhe ekonominë. Me zhvillimet teknologjike globale të viteve të fundit siguria kibernetike është kthyer në prioritet dhe për qeverinë shqiptare. Zhvillimi i kësaj fushe ka marrë një rëndësi të veçantë për shoqërinë dhe ekonominë, duke konsideruar numrin e lartë të shërbimeve që sot ofrohen online dhe çështje të tjera të rëndësishme si më poshtë

Zhvillimi i infrastrukturës së nevojshme në fushën e teknologjisë së informacionit dhe komunikimit: Shqipëria i ka dhënë rëndësi modernizimit dhe zhvillimit të infrastrukturës së nevojshme në fushën e teknologjisë së informacionit dhe komunikimit, duke përfshirë përdorimin e teknologjive të avancuara të informacionit. Digjitalizimi i shërbimeve publike me qëllim efikasitetin dhe kualitetin e dhënies së shërbimit dhe ndërveprimit midis qeverisë, qytetarëve dhe biznesit është një nga proceset më të rëndësishme që ka ndodhur në vend. Këto zhvillime kanë rritur ekspozimin ndaj kërcënimeve të ndryshme kibernetike, duke sjellë nevojën emergjente për të ndërmarrë masa konkrete për të siguruar infrastrukturat e informacionit.

Kërcënimet kibernetike:
Ashtu si në shumë vende të tjera edhe Shqipëria po përballet me një numër të lartë të kërcënimeve kibernetike. Këto kërcënime përfshijnë sulmet ndaj infrastrukturave kritike dhe të rëndësishme të informacionit duke shenjëstruar institucionet qeveritare dhe kompanitë private.
Për shkak të nevojës për mbrojtjen e të dhënave personale dhe garantimin e funksionimit të duhur të sistemeve dhe rrjeteve të informacionit, siguria kibernetike ka marrë një rëndësi të veçantë duke qenë e lidhur ngushtë me sigurinë kombëtare.

Identifikimi i Infrastrukturave Kritike dhe të Rëndësishme të Informacionit:
Identifikimi i infrastrukturave kritike dhe të rëndësishme të informacionit është një hap i rëndësishëm për sigurinë kibernetike dhe mbrojtjen e sistemeve që ruajnë dhe përpunojnë të dhënat (Crown Jewels), mosfunksionimi i të cilave mund të shkaktojë pasoja të rënda në nivel kombëtar.
Në Shqipëri janë identifikuar **289** infrastruktura kritike dhe të rëndësishme të informacionit në sektorët: bankar, financiar, energjetik, transport, shëndetësor, infrastrukturat digjitale dhe furnizimin me ujë.
Gjithashtu, AKCESK është në proces identifikimi të infrastrukturave të reja kritike dhe të rëndësishme të informacionit, duke përfshirë edhe institucionet e sigurisë dhe mbrojtjes.

Rëndësia në ekonomi dhe shoqëri: Siguria kibernetike luan rol të rëndësishëm në ekonomi pasi shumë sektorë përdorin teknologjitë e informacionit dhe komunikimit për të ofruar shërbimet e tyre. Sulme të mundshme kibernetike mund të shkaktojnë dëme të mëdha ekonomike, pasi mund të prekin sektorët kritik si ai bankar, financiar, energjetik, transport, shëndetësor, infrastrukturat digjitale, furnizimin me ujë, apo dhe kompanitë e tjera të rëndësishme.
Ndërgjegjësimi dhe edukimi i publikut në lidhje me mënyrat e mbrojtjes së sigurisë kibernetike kanë një ndikim të rëndësishëm në reduktimin e problematikave të sigurisë kibernetike.

Mbrojtja Kibernetike: Mbrojtja kibernetike është një çështje globale që po bëhet gjithnjë e më e rëndësishme dhe përfshin marrjen e masave për mbrojtjen e sistemeve dhe rrjeteve të informacionit në infrastrukturat kritike dhe të rëndësishme si dhe garantimin e sigurisë së të dhënave sensitive nga sulmet dhe kërcënimet e ndryshme kibernetike.
Shqipëria po zhvillon kapacitetet teknike dhe njerëzore në fushën e sigurisë kibernetike, duke u përgatitur për sfidat e kohës së re digjitale.

II. KUADRI LIGJOR DHE RREGULLATOR

AKCESK është krijuar me VKM Nr. 141, datë 22.2.2017, ka përgjegjësinë e mbikëqyrjes së zbatimit të Ligjit Nr.9880/2008, "Për Nënshkrimin Elektronik", Ligjit Nr.107/2015, "Për Identifikimin Elektronik dhe Shërbimet e Besuara" si dhe Ligji Nr. 2/2017, "Për Sigurinë Kibernetike" dhe të akteve nënligjore të nxjerra në zbatim të tyre.
Krijimi i AKCESK ishte një hap i rëndësishëm për të adresuar sfidat e sigurisë kibernetike në nivel kombëtar dhe për të ndihmuar në koordinimin e përgjegjësive dhe veprimeve në këtë fushë.

Ligji Nr. 2/2017, "Për Sigurinë Kibernetike", është ligji i parë i miratuar në vend që mbulon çështjet e sigurisë kibernetike i transponuar pjesërisht nga *Direktiva e BE NIS 1.*

Qëllimi i këtij ligji është arritja e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellë ndërmjet subjekteve që operojnë në fushën e sigurisë kibernetike.

Aktet nënligjore të nxjerra në zbatim të Ligjit Nr.2/2017, "Për sigurinë kibernetike", janë:

- VKM Nr. 141, datë 22.2.2017, "Për organizimin dhe funksionimin e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike", e ndryshuar, ku përcaktohen funksionet dhe përgjegjësitë e Autoritetit.
- VKM Nr. 553, datë 15.07.2020, "Për miratimin e Listës së Infrastrukturave Kritike të Informacionit dhe të Listës së Infrastrukturave të Rëndësishme të Informacionit", e ndryshuar.
- Rregullore "Mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë", miratuar me (Versioni 2.0)
- Rregullore "Për Kategoritë e Incidenteve Kibernetike si dhe formatin dhe elementët e raportit"
- Udhëzim "Për Metodologjinë e Organizimit dhe Funksionimit të CSIRT-eve në Nivel Kombëtar"
- VKM Nr. 1084, datë 24.12.2020, "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe Planit të veprimit 2020-2025"

Aktualisht është miratuar i **Ligji i ri** për sigurinë kibernetike në përputhje të plotë me Direktivën e BE-së, *"Në lidhje me masat për një nivel të lartë të përbashkët të sigurisë së rrjeteve dhe sistemeve të informacionit në të gjithë Bashkimin Evropian" (NIS 2),* detyrim ky edhe në kuadër të Planit Kombëtar të Integrimit Evropian të Republikës së Shqipërisë 2022-2025.

Duke konsideruar që vendet anëtare të BE-së kanë afat deri në tetor të vitit 2024 për ta transpozuar dhe implementuar në legjislacionet kombëtare përkatëse këtë direktivë, Shqipëria ka bërë hapa përpara në integrimin e dispozitave të direktivës NIS2 në kornizën ligjore kombëtare përmes miratimit te këtij Ligji.

III. POLITIKA DHE STRATEGJITË E SIGURISË KIBERNETIKE

Qëllimi i Politikave të sigurisë kibernetike është rishikimi dhe koordinimi i detyrimeve që lindin nga angazhimet e marra për një hapësirë kibernetike të sigurt në nivel kombëtar që të sigurohet përmbushja e përgjegjësive nga të gjithë aktorët.

Objektivat kryesore të politikave të sigurisë kibernetike bazohen në tre shtylla kryesore:

1. Burime njerëzore: Rritja e ndërgjegjësimit dhe aftësimit për sigurinë kibernetike në të gjithë organizatën për të siguruar që të gjithë përdoruesit të njohin praktikat e sigurta, identifikojnë kërcënimet kibernetike dhe raportojnë sjellje të dyshimta. Kjo nënkupton trajnime të rregullta, simulime të sulmeve kibernetike, si dhe udhëzime të qarta mbi standardet e sigurisë duke rritur aftësitë profesionale për të implementuar masat e sigurisë kibernetike dhe për tu përgjigjur në mënyrë efektive ndaj sulmeve kibernetike.

2. Procese: Zbatimi i politikave dhe procedurave të qarta për mbrojtjen e të dhënave, zbulimin dhe përgjigjen ndaj incidenteve kibernetike, si dhe rishikimin e rregullt të këtyre proceseve për t'u përshtatur me kërcënimet e reja. Kjo përfshin krijimin e një plani reagimi ndaj incidenteve kibernetike dhe kontrolle të rregullta të përputhshmërisë me standardet e sigurisë.

3. Teknologjia: Implementimi i teknologjive të sigurta për mbrojtjen e të dhënave, zbulimin e kërcënimeve kibernetike dhe reduktimin e ekspozimit ndaj rreziqeve. Kjo nënkupton përdorimin e sistemeve të monitorimit, autentikimit të avancuar, enkriptimin e të dhënave dhe pajisjeve të dedikuara për parandalimin e sulmeve kibernetike.

Pas sulmit kibernetik të sofistikuar të ndodhur në vitin 2022, ndaj infrastrukturave kritike të informacionit në Shqipëri, AKCESK u riorganizua për të përmbushur vizionin e qeverisë shqiptare për të arritur një nivel të lartë të sigurisë kibernetike në vend. Kjo riorganizim u shoqërua me një rritje të numrit të punonjësve nga 24 në 85, duke i dhënë AKCESK kapacitetet e nevojshme teknologjike dhe njerëzore për të adresuar sfidat e sigurisë kibernetike.

STRATEGJIA KOMBËTARE PËR SIGURINË KIBERNETIKE 2020-2025

Me qëllim forcimin e sigurisë kibernetike në nivel kombëtar dhe garantimin e një ekosistemi të sigurt dhe të qëndrueshëm kibernetik në Shqipëri, Qeveria shqiptare ka miratuar me Vendimit të Këshillit të Ministrave Nr. 1084, datë 24.12.2020, Strategjinë Kombëtare për Sigurinë Kibernetike dhe Planin e Veprimit 2020-2025.

Strategjia bazohet në katër shtylla kryesore:

1. **Garantimi** i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike.
2. **Ndërtimi** i një mjedisi të sigurt kibernetik, duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit.
3. **Krijimi** i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin e ri, të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit.
4. **Rritje** e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjikë.

Në funksion të realizimit të objektivave strategjike, Shqipëria punon për zgjerimin e marrëveshjeve bilaterale dhe multilaterale në fushën e sigurisë kibernetike me partnerë ndërkombëtare, si dhe është përfshirë në aktivitetet dhe partneritetet ndërkombëtare për të ndarë informacione dhe praktikat më të mira në fushën e sigurisë kibernetike.

Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025, parashikon nevojën e rishikimit të Planit të Veprimit çdo dy vjet, bazuar në dinamikën e zhvillimit të sektorit të sigurisë kibernetike. AKCESK ka punuar intensivisht për rishikimin e Planit të Veprimit 2020-2025 dhe ka hartuar Planin e Veprimit 2024-2025, duke identifikuar prioritetet dhe nevojat si dhe duke u koordinuar me institucionet përgjegjëse sa i përket zbatimit të tij.

Në Planin e Veprimit të rishikuar për periudhën 2024-2025, janë përcaktuar masa konkrete që do të bëjnë të mundur adresimin e nevojave, prioriteteve dhe përshpejtimin e progresit për sigurinë kibernetike.

Plani i Veprimit 2024-2025, do të kontribuojë për të arritur rezultatet e mëposhtme të synuara edhe nga Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025:

- **Përmirësimi i kornizës politike dhe ligjore**, duke përfshirë ligjet, politikat strategjike, rregulloret, metodologjitë dhe procedurat, përmes implementimit të politikave dhe standardeve të sigurisë kibernetike të BE-së gjithashtu.
- **Fuqizimi i strukturave dhe infrastrukturave të sigurisë kibernetike** në lidhje me kapacitetet teknike dhe profesionale si dhe procedurat e tyre përkatëse. Kjo u realizua përmes ngritjes së Qendrës Kombëtare Operacionale të Sigurisë Kibernetike (SOC) për monitorimin dhe trajtimin e incidenteve të sigurisë kibernetike, ngritjes së laboratorëve të analizimit të programeve keqdashëse (malware), hetimit kibernetik dhe simulimit të incidenteve kibernetike, rritjes së kapaciteteve teknike dhe profesionale, analizës teknologjike të mjedisit të infrastrukturave kritike, përmirësimi i procedurave të trajtimit dhe menaxhimit të incidenteve dhe të tjera, të cilat parashikohen në planin e veprimit.
- **Rritja e ndërgjegjësimit dhe edukimi**, si dhe përmirësimi i masave parandaluese dhe mbrojtëse në lidhje me kërcënimet e sigurisë kibernetike, krimin kibernetik dhe përmbajtjet e paligjshme në internet, sigurinë dhe mbrojtjen e fëmijëve në internet, si dhe ekstremizmin e dhunshëm dhe radikalizmin në hapësirën kibernetike.
- **Rritja e kapaciteteve profesionale në sigurinë kibernetike** përmes organizimit të trajnimeve dhe certifikimeve, në bashkëpunim me partneret kombëtar dhe ndërkombëtar.
- **Forcimi i bashkëpunimit kombëtar dhe ndërkombëtar**, ku janë planifikuar disa aktivitete, të tilla si: krijimi i një forumi me institucione publike dhe private në Shqipëri dhe agjenci ndërkombëtare, krijimi i një strukture të diplomacisë kibernetike në Ministrinë për Evropën dhe

Punët e Jashtme në koordinim me AKCESK, hartimi dhe nënshkrimi i marrëveshjeve dypalëshe dhe shumëpalëshe në fushën e sigurisë kibernetike, promovimi dhe zbatimi i ligjit ndërkombëtar, normave dhe masave të ndërtimit të besimit në lidhje me sjelljen e përgjegjshme të shtetit në hapësirën kibernetike, pjesëmarrje aktive në OKB, NATO, OSBE, BE dhe organizata të tjera ndërkombëtare, stërvitje rajonale kibernetike, pjesëmarrje në projekte ndërkombëtare, etj.

Plani i Veprimit 2024-2025, kontribuon gjithashtu në procesin e integrimit evropian të Shqipërisë, pasi parashikon aktivitete në lidhje me përmirësimin e kuadrit ligjor dhe të politikave aktuale nëpërmjet zbatimit të politikave të BE-së, standardeve të sigurisë kibernetike dhe praktikave më të mira, si dhe bashkëpunimit ndërkombëtar me partnerët strategjikë.

INSTITUCIONET PËRGJEGJËSE PËR SIGURINË KIBERNETIKE

AKCESK si institucioni përgjegjës dhe mbikëqyrjes për zbatimin e legjislacionit në fuqi për sigurinë kibernetike në Shqipëri luajnë rol kyç për hartimin, menaxhimin dhe zbatimin e politikave të sigurisë kibernetike.

Rolet dhe përgjegjësitë e AKCESK:

- Vepron në cilësinë e Ekipit Kombëtar të Përgjigjes ndaj Incidenteve të Sigurisë Kompjuterike (CSIRT Kombëtar).
- Vepron si pikë qendrore kontakti në nivel kombëtar për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe koordinon punën për zgjidhjen e incidenteve të sigurisë kibernetike.
- Menaxhon Qendrën Kombëtare Operacionale të Sigurisë (SOC) e cila monitoron aktivitetet keqdashëse në infrastrukturat kritike dhe të rëndësishme të informacionit dhe trajton incidentet kibernetike.
- Harton politika strategjike, rregullore, plane dhe procedura me qëllim forcimin e sigurisë kibernetike në nivel kombëtar dhe monitoron zbatimin e tyre.
- Ushtron rolin e koordinatorit në nivel kombëtar në bashkëpunim me të gjitha institucionet përkatëse për zbatimin dhe monitorimin e "Strategjisë Kombëtare për Sigurisë Kibernetike".
- Identifikon dhe klasifikon infrastrukturat kritike dhe të rëndësishme të informacionit dhe garanton mbrojtjen e tyre.
- Përcakton masat e sigurisë kibernetike dhe mbikëqyr/kontrollon zbatimin e tyre.
- Koordinon veprimet e të gjitha strukturave përgjegjëse për zgjidhjen e situatave të krizave kibernetike.
- Zhvillon programe dhe politika specifike për rritjen e ndërgjegjësimit për sigurinë kibernetike në nivel kombëtar.
- Bashkëpunon me organizata dhe partnerë ndërkombëtarë në fushën e sigurisë kibernetike me qëllim shkëmbimin e praktikave dhe ekspertizës më të mirë, ndërtimin e kapaciteteve, shkëmbimin e informacionit dhe zbatimin e projekteve të përbashkëta.

Gjithashtu, institucionet e tjera përgjegjëse për implementimin e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike të rishikuar 2024-2025, janë si më poshtë:

- Ministria e Arsimit dhe Sportit;
- Ministria e Shëndetësisë dhe Mbrojtjes Sociale;
- Qendra e Koordinimit kundër Ekstremizmit të Dhunshëm;
- Ministria e Infrastrukturës dhe Energjisë;
- Agjencia Kombëtare për Shoqërinë e Informacionit;
- Drejtoria e Përgjithshme e Policisë së Shtetit;
- Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar;
- Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP): AKEP ka rol në monitorimin dhe rregullimin e sektorit të telekomunikacionit dhe mbikëqyrjen e sigurisë kibernetike në këtë sektor.
- Ministria për Evropën dhe Punët e Jashtme.

Objektivat kryesore ku do të mbështetet ACESK dhe institucionet përgjegjëse për implementimin e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike të rishikuar 2024-2025 janë si më poshtë:

Objektivi Specifik	Nën objektivat	Institucioni përgjegjës
Objektivi Specifik A - Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i tij me direktivat dhe rregulloret e Bashkimit Evropian.	**A.1** Përmirësimi i kuadrit rregullator për sigurinë kibernetike i harmonizuar me ligjet sektoriale, për të adresuar saktë çështjet dhe zgjidhur ato duke përfshirë, por pa u kufizuar: Cloud computing, ICT, teknologjinë 5G, Inteligjencën Artificiale.	AKCESK/ MIE/AKEP/ MD/MB/PSH
	A.2.Përshtatja e vazhdueshme e standardeve dhe rregullave sipas zhvillimeve të fushës, së sigurisë kibernetike.	
	A.3. Përmbushja e angazhimeve të marra si vend i Aleancës së Atlantikut të Veriut, për hapësirën kibernetike.	PSH/ AKCESK
	A.4. Përcaktimi i një procedure kombëtare për rastet e gjendjeve të jashtëzakonshme të krijuar nga krizat kibernetike, me qëllim marrjen e masave konkrete për zgjidhjen e situatës në kohe reale.	AKCESK
Objektivi Specifik B - Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar	**B.1.** Ngritja e CSIRT-it Kombëtar dhe CSIRT-ve të reja sektoriale, në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe fuqizimi i atyre ekzistuese	AKCESK/ AKSHI/ PSH/ MIE/AKEP/ AKESK
	B.2. Krijimi i kushteve optimale të punës për funksionimin e CSIRT-eve, në përmbushje të detyrave të veta, për të garantuar sigurinë kibernetike në infrastrukturat kritike e të rëndësishme të informacionit.	AKCESK/ AKSHI/ PSH/ MIE/AKEP
	B.3. Ngritja e kapaciteteve të CSIRT-eve, nëpërmjet trajnimeve dhe stërvitjeve kibernetike.	AKCESK/ AKSHI/ PSH/ MIE/ AKEP
	C.1. Përdorimi i zgjidhjeve hardware dhe software të avancuara për identifikimin, parandalimin, dhe menaxhimin e incidenteve kibernetike.	AKCESK/ AKSHI/PSH
	C.2. Analizimi i infrastrukturave kritike dhe të rëndësishme të informacionit për vlerësimin e menaxhimin e riskut në to.	AKCESK/ AKSHI
	C.3. Hartimi i planeve strategjike për mbrojtjen e hapësirës kibernetike nga incidente të mundshme.	AKCESK
	C.4 Realizimi i vetëvlerësimeve në Infrastrukturat kritike dhe të rëndësishme të informacionit për matjen e nivelit të maturimit të sigurisë kibernetike.	AKCESK

Objektivi Specifik D - Përmirësimi i infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizmin dhe ekstremizmin e dhunshëm	**D.1.** Monitorimi dhe parandalimi i fenomeneve, që nxisin ekstremizmin e dhunshëm dhe radikalizmin në shtresat vulnerabël në hapësirën kibernetike	CVE
	D.2 Evidentimi në vazhdimësi i elementeve kontaminues, që qarkullojnë në Internet, që cenojnë sigurinë kibernetike në vend	PSH/ AKCESK
	D.3 Ngritja e mekanizmave për rregullimin e Internetit të sigurt në ambientet publike, të certifikuar nga autoriteti rregullues i fushës së sigurisë kibernetike	AKCESK
	D.4 Ngritja e kapaciteteve të autoriteteve përgjegjëse kundër krimit kibernetik.	AKCESK/ PSH/ AKSHI
	D.5 Rritja e bashkëpunimit rajonal në luftën kundër krimit kibernetik	PSH
Objektivi Specifik A - Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore	**A.1** -Hartimi i programeve studimore në arsimin e lartë në fushën e sigurisë kibernetike, me qëllim krijimin e gjeneratës së re të ekspertëve të sigurisë kibernetike	AKCESK
	A.2. Hartimi i rekomandimeve për integrimin në kurrikula universitare të informacioneve në lidhje me Internetin e Sigurt.	AKCESK/ MAS
	A.3. Rritja e kapaciteteve kërkimore dhe inovative në fushën e sigurisë kibernetike	AKCESK/ MAS/ UNIVERSITETET
Objektivi Specifik B - Rritja e ndërgjegjësimit dhe e aftësive profesionale të institucioneve publike dhe private për sigurinë kibernetike.	**B.1.** Trajnime periodike, për thellimin e njohurive në sigurinë kibernetike, sipas dinamikës së fushës, për stafin administrativ në nivel qendror dhe në nivel lokal	AKCESK
	B.2. Rritja dhe mbështetja e kapaciteteve kërkimore dhe risive të biznesit nëpërmjet nxitjes së ngritjes së qendrave kërkimore shkencore në fushën e sigurisë kibernetike	AKCESK
	B.3. Rritja e kapaciteteve të CSIRT-eve në nivel kombëtar dhe nivelit ekzekutiv të administratës publike nëpërmjet trajnimeve dhe stërvitjeve kibernetike	AKCESK/ AKSHI
Objektivi Specifik C - Rritje e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe kërcënimet kibernetike.	**C.1** Rritja e ndërgjegjësimit të shoqërisë për sigurinë kibernetike, duke përdorur hapësirat e duhura për realizimin e tyre, përfshirë edhe mediat audiovizive apo edhe ato sociale	AKCESK
	C.2 Krijimin e një platforme edukative online, për sigurinë kibernetike, për të rritur ndërgjegjësimin në grup mosha të ndryshme të shoqërisë, për përdorimin e Internetit të sigurt dhe të infrastrukturës digjitale	AKCESK/ ASHMDF/ MAS/ AKSHI/ PSH/AKEP etj.
Objektivi Specifik A - Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në Internet.	A.1 Hartimi i një udhëzimi të posaçëm (dhe rregullores shoqëruese) për mbledhjen e të dhënave të incidenteve të raportuara të dhunës, bullizimit dhe abuzimit online të fëmijëve në shkolla.	MAS/ AKCESK
	A.2. Përmirësimi i kuadrit rregullator për ta sjellë në linjë me legjislacionin ndërkombëtar për mbrojtjen e fëmijëve nga abuzimi seksual në Internet	MAS/ ASHDMF/ PSH
	A.3. Plotësimi dhe qartësimi i legjislacionit në lidhje me njoftimin, heqjen dhe bllokimin e materialeve të paligjshme online	AKCESK/ PSH/ AKEP
Objektivi Specifik B - Parandalimi i abuzimit seksual të fëmijëve në Internet nëpërmjet rritjes së ndërgjegjësimit dhe krijimit të hapësirave të sigurta për lundrimin në Internet	**B.1.** Integrimi i programit 'Edukatorët bashkëmoshatarët për sigurinë online'' në sistemin edukativ	MAS
	B.2. Krijimi dhe mbështetja e rrjetit online të mësuesve të TIK për të promovuar çështjen e mbrojtjes së fëmijëve në Internet	MAS/AKCESK
	B.3 Krijimi i hapësirave publike me internet të sigurtë për fëmijët dhe familjet nëpërmjet nismës 'Friendly Wi-Fi' në 5 Bashki të vendit, duke ofruar jo vetëm aksesim falas të internetit por njëkohësisht informacion të filtruar me qëllim mbrojtjen e fëmijëve dhe të rinjve nga përmbajtjet abuzuese online.	AKCESK

	B.4 Aplikimi i filtrave në shkollat publike dhe private për të parandaluar aksesin e fëmijëve në faqe të papërshtatshme dhe të paligjshme si dhe informimi në vijueshmëri i mësuesve të TIK për raportimin e incidenteve.	MAS/AKCESK
	B.5 Identifikimi, mbështetja dhe promovimi i talenteve për të krijuar zgjidhje teknike që ndihmojnë në mbrojtjen dhe sigurinë online.	MAS/AKCESK/MSHRF
Objektivi Specifik C - Hetimi efektiv dhe sjellja para drejtësisë e autorëve të krimeve kibernetike ndaj fëmijëve, me fokus abuzimin dhe shfrytëzimin seksual	**C.1.**Sigurimi i mjeteve teknike që ndihmojnë policinë dhe organet përkatëse në analizimin dhe zbulimin e rasteve të dhunës online veçanërisht lidhur me imazhet e abuzimit seksual me fëmijët	AKCESK/ ASHDMF/ PSH/AKEP/MSHMS/ ASHDM
	C.2. Krijimi i programeve të trajnimit për personelin e gjyqësorit, prokurorisë dhe Policisë në lidhje me mbrojtjen e fëmijëve në Internet dhe sigurinë kibernetike, duke përfshirë evidenca të përdorimit digjital dhe ndihmën e ndërsjelltë juridike	AKCESK/ PSH
	C.3. Ngritja e një sistemi kursesh pranë Shkollës se Magjistraturës dhe Akademisë së Sigurisë në lidhje me çështjet që kanë të bëjnë më krimet ndaj fëmijëve online dhe mënyrat e mbrojtjes së tyre në Internet.	AKCESK
	C.4 Krijimi i mekanizmave për standardizimin e punës së analizimit të provave digjitale nga Policia e Shtetit.	PSH
	C.5 Krijimi i një grupi pune së bashku me industrinë për të zgjidhur problemet e hetimit dhe identifikimit të personave të dyshuar për abuzim me fëmijët online, me fokus të veçantë identifikimin e përdoruesve fundorë nëpërmjet adresave IP.	PSH/ ASHDMF/ AKCESK/ AKEP
Objektivi Specifik D - Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurt të Internetit nga fëmijët	**D.1** Fushata ndërgjegjësimi me prindërit dhe edukatorët në lidhje me rreziqet dhe problemet me të cilat përballen fëmijët në Internet	AKCESK/ ASHMDF/ MAS/ZVA
	D.2 Zhvillimi i programeve të trajnimit me mësuesit e TIK në lidhje me çështjet e internetit të sigurtë	AKCESK/ MAS
	D.3 Zhvillimi i programeve të trajnimit për Punonjësit e Mbrojtjes së Fëmijës lidhur me trajtimin e rasteve të fëmijëve në nevojë për mbrojtje ku rreziku i dhunës, abuzimit, shfrytëzimit apo neglizhimit lidhet me internetin dhe teknologjitë e informacionit	AKCESK/ MSHMS/ ASHDMF
Objektivi Specifik E - Forcimi i bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në Internet.	**E.1.** Promovimi nëpërmjet bashkëpunimit me të gjitha ISP-të i mekanizmave ekzistues të aplikuar në platformat e tyre për sigurinë e fëmijëve në Internet.	AKCESK/ AKEP/ ISP/ ASHDMF
	E.2 Integrimi nga të gjitha ISP-të në platformat e tyre të Listës IWF (Internet watch Foundation Hash List) që ndalon çdo individ të hedhë, shkarkojë apo shikojë imazhe apo video të abuzimit seksual të fëmijëve	AKCESK
	E.3 Ngritja e një Komiteti Teknik Këshillues për Sigurinë e Fëmijëve në Internet, pranë Këshillit Kombëtar për të Drejtat dhe Mbrojtjen e Fëmijëve	MSHMS
Objektivi Specifik A - Forcimi i bashkëpunimit institucional në nivel kombëtar	**A.1.** Rritja e bashkëpunimit dhe koordinimit ndërmjet institucioneve shtetërore për të garantuar sigurinë në nivel kombëtar në hapësirën kibernetike	MEPJ/ AKCESK
	A.2. Krijimi i një instrumenti për shkëmbimin e informacionit përmes pikave të kontaktit të dedikuara nga institucionet përkatëse, në raste të kërcënimeve kibernetike.	AKCESK
	A.3. Ngritja e një strukture fleksibël me ekspertët më të mirë të sigurisë kibernetike në vend, me qëllim mbështetje në raste krizash kibernetike, testimi dhe vlerësimi të nivelit të sigurisë kibernetike në nivel kombëtar	AKCESK
Objektivi Specifik B -Forcimi i bashkëpunimit	**B.1.** Zhvillimi i mekanizmave dhe procedurave efikase, për bashkëpunim ndërkombëtar, në rast të incidenteve kibernetike, sulmeve dhe krizave, sipas parimeve të vendosura ndërkombëtarisht.	MEPJ/ AKCESK

ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizmit	**B.2**. Forcimi i bashkëpunimit dhe shkëmbimi i informacionit me NATO / OSBE dhe organizata / forume të tjerë ndërkombëtarë	AKCESK,MEPJ/.etj.

Këto institucione janë të koordinuara dhe bashkëpunojnë për të ndërmarrë masa për të forcuar sigurinë kibernetike në vend. Rëndësi të veçantë ka bashkëpunimi i ngushtë midis këtyre institucioneve dhe ndarja e informacioneve dhe përvojave për të përballuar sfidat e sigurisë kibernetike në mënyrë efektive.

IV. QEVERISJA E SIGURISË KIBERNETIKE

Politikat e sigurisë kibernetike përfshijnë përdorimin e qeverisjes kibernetike si një instrument i rëndësishëm për përmirësimin e qeverisjes dhe ofrimin e shërbimeve publike në mënyrë më efikase, transparente dhe të sigurt.
Përdorimi i teknologjisë së informacionit në administratën publike ka potencialin për të përmirësuar qëndrueshmërinë ekonomike si dhe cilësinë e jetës së qytetarëve në Shqipëri. Megjithatë, është thelbësore që të sigurohet që këto platforma të jenë të sigurta dhe të mbrohen nga kërcënime kibernetike për të garantuar integritetin dhe konfidencialitetin e të dhënave qeveritare dhe personale të qytetarëve.

Politika e rrezikut kibernetik kombëtar do të mundësojë vlerësimin e rrezikut kibernetik duke identifikuar dhe prioritizuar kërcënimet dhe cënueshmëritë ndaj sigurisë kibernetike me qëllim reduktimin e rrezikut, marrjen e masave parandaluese dhe reaguese në kohë, si dhe garantimin e qëndrueshmërisë kibernetike.

Politikat e monitorimit dhe vlerësimit të performancës do të bëjë të mundur përcaktimin e kornizës së duhur politike për realizimin e monitorimit dhe vlerësimit të nivelit dhe qëndrueshmërisë së sigurisë kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit për të garantuar që të jenë sa më të mbrojtura dhe të pacënueshme nga kërcënimet e mundshme nga aktorë keqdashës.

Politika e krizës kibernetike, si një kornizë gjithëpërfshirëse e projektuar për të përcaktuar procedurën e menaxhimit të krizës kibernetike dhe përgjigjen në nivel kombëtar ndaj incidenteve kibernetike që mund të përshkallëzohen në kriza kombëtare, shërben për të forcuar përgatitjen, menaxhimin efektiv dhe rikuperimin nga të tilla incidente.

Politika e komunikimit përcakton si duhet të realizohet komunikimi në nivel kombëtar në lidhje me kërcënimet kibernetike, incidentet, ndërgjegjësimin dhe bashkëpunimin, duke përfshirë komunikimin e brendshëm, komunikimin publik, komunikimin e krizës, dhe komunikimin lidhur me bashkëpunimet kombëtare dhe ndërkombëtare.

Politika për rritjen e kapaciteteve të institucioneve për sigurinë kibernetike ka për qëllim adresimin e sfidave sa i përket kapaciteteve teknike dhe njerëzore të institucioneve publike dhe private në nivel kombëtar duke parashikuar masat që duhet të ndërmerren për rritjen e kapaciteteve njerëzore, kapaciteteve teknike, si dhe për krijimin e mekanizmave të nevojshëm dhe rritjen e bashkëpunimit

kombëtar dhe ndërkombëtar, në funksion të ngritjes dhe forcimit të kapaciteteve, me qëllim forcimin e sigurisë kibernetike.

Politika e partneritetit publik-privat është një qasje strategjike që lehtëson bashkëpunimin midis institucionit, organizatave dhe subjekteve të sektorit privat për të forcuar sigurinë kombëtare kibernetike në vend. Ky bashkëpunim dhe fitimi i besimit mes institucionit dhe subjekteve private mund të realizohet nëpërmjet vendosjes së një platforme formale për komunikim dhe bashkëpunim të vazhdueshëm në fushën e sigurisë kibernetike. Ky bashkëpunim mund të forcohet gjithashtu nëpërmjet zhvillimit të projekteve në fusha si mbrojtja e infrastrukturës kritike, kërkimi dhe zhvillimi, ose fushatat e ndërgjegjësimit, programeve të përbashkëta të trajnimit të ekspertëve dhe stërvitjeve për të ndërtuar aftësitë dhe ekspertizën në sigurinë kibernetike. Inkurajimi për adoptimin e standardeve kombëtare dhe ndërkombëtare të sigurisë kibernetike dhe praktikave më të mira në përgjigje ndaj incidenteve dhe planeve të rikuperimit për të menaxhuar dhe zbutur ndikimin e incidenteve kibernetike dhe për të pasur një përgjigje më të koordinuar ndaj kërcënimeve kibernetike në sektorin privat.

Politika e menaxhimit të incidenteve është një kornizë politike e hartuar për të mundësuar trajtimin me efektivitet të incidenteve e cila përfshin objektivat dhe masat që duhen realizuar për menaxhimin e suksesshëm të incidentit në mënyrë që të minimizohet ndikimi sa më shumë të jetë e mundur dhe të parandalohet përshkallëzimi i mëtejshëm.

Politika e mbrojtjes së fëmijëve në hapësirën kibernetike është një politikë që parashikon objektivat dhe masat e nevojshme për të edukuar, informuar dhe mbrojtur fëmijët nga rreziqet në internet, me qëllim garantimin e një hapësire kibernetike të sigurt për fëmijët në Shqipëri.

Politika për mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit është një politikë që përfshin hapat dhe masat që duhen marrë duke filluar që nga procesi i identifikimit të tyre, vlerësimi i rrezikut kibernetik, përcaktimi i standardeve të sigurisë kibernetike që duhet të aplikohen në këto infrastruktura, e deri te planet për rritjen e kapaciteteve teknike dhe njerëzore të operatorëve të tyre në fushën e sigurisë kibernetike.

Politika për ndërgjegjësimin mbi sigurinë kibernetike ka si qëllim krijimin e një shoqërie të ndërgjegjësuar në lidhje me sigurinë kibernetike në Shqipëri, duke përfshirë të gjithë aktorët në çdo sektor dhe përcaktuar masat që bëjnë të mundur rritjen e ndërgjegjësimit mbi kërcënimet e sigurisë kibernetike dhe mënyrat e mbrojtjes ndaj rreziqeve të mundshme në internet.

Këto politika do të kontribuojnë për të forcuar sigurinë kibernetike në Shqipëri duke forcuar masat parandaluese, menaxhuese dhe reaguese në lidhje me kërcënimet kibernetike.

Politika për barazinë gjinore ka rëndësi për të siguruar barazi dhe diversitet në vendin e punës. Ajo përfshin politikat që inkurajojnë dhe mbështesin të dy gjinitë në të gjitha nivelet. Kjo përfshin qasja të barabarta në rekrutim, pagesa dhe punë të barabarta, programe trajnimi dhe zhvillimi.

QEVERISJA E SIGURISË KIBERNETIKE SIPAS SEKTORËVE

Vlerësimi i qeverisjes së sigurisë kibernetike në rang kombëtar bazohet në principet e mëposhtme:

ROLET DHE PËRGJEGJËSITË

Për të arritur një qeverisje efektive të sigurisë kibernetike, është e nevojshme përcaktimi i qartë i roleve dhe përgjegjësive të secilit person ose sektor për çështjet e sigurisë kibernetike. Kjo siguron që çdo person ose ekip të jetë në dijeni nëpërmjet një procedure të miratuar të detyrave dhe përgjegjësive dhe të punojë për përmbushjen e objektivave të përgjithshme të sigurisë kibernetike të institucionit ku bën pjesë.

Disa hapa të rëndësishëm për të arritur këtë janë:

1. **Përcaktimi i roleve të sigurisë kibernetike:** Çdo subjekt apo institucion i cili administron infrastruktura kritike apo të rëndësishme të informacionit, duhet të identifikojë rolet specifike për sigurinë kibernetike. Kjo përfshinë rolin e shefit të sigurisë së informacionit, oficerit të sigurisë së informacionit, oficerit të mbrojtjes së të dhënave, administratorit të sistemeve të informacionit, etj.
2. **Krijimi i një strukture organizative të dedikuar për sigurinë kibernetike:** Kjo strukturë e posaçme përfshin departamentet ose sektorët e specializuar të sigurisë kibernetike (CSIRT Sektorial)
3. **Përcaktimi i detyrave dhe përgjegjësive**: Përcaktohen detyrat dhe përgjegjësitë specifike të secilit rol të sigurisë kibernetike, duke përfshirë monitorimin, zbulimin, parandalimin dhe menaxhimin e incidenteve kibernetike.
4. **Komunikimi dhe ndërgjegjësimi**: Rëndësi të veçantë ka që i gjithë personeli të kuptojë detyrat dhe përgjegjësitë e tyre në fushën e sigurisë kibernetike, pasi secili kontribuon në mbrojtjen e sistemeve dhe rrjeteve të informacionit ku bën pjesë.
5. **Përmirësimi i politikave dhe rregulloreve**: Politikat dhe rregulloret për sigurinë kibernetike rishikohen periodikisht, në bazë të ndryshimeve të përcaktuara në rolet dhe përgjegjësitë.
6. **Auditimi dhe rishikimi menaxherial:** Auditimet dhe rishikimi menaxherial për të vlerësuar efektivitetin e roleve dhe përgjegjësive të sigurisë kibernetike si dhe efektivitetin e sistemit te menaxhimit të sigurisë se informacionit
7. **Trajnimet dhe ngritja e kapaciteteve njerëzore**: Trajnimet e vazhdueshme, si dhe zhvillimi profesional për personelin e sigurisë kibernetike për të rritur më tej aftësitë e tyre.

Në subjekte më të vogla, disa role të sigurisë kibernetike mund të përfshihen në detyrën e një personi të vetëm. Në raste të tilla, është akoma më e rëndësishme që bordi i lartë menaxhues të sigurojë që detyrat e sigurisë kibernetike të kuptohen qartë dhe të komunikohen mirë. Të gjithë në organizatë duhet të kuptojnë rolin e tyre në mbështetjen e sigurisë kibernetike efektive.

AKCESK, për t'ju ardhur në ndihmë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për krijimin e CSIRT-eve sektoriale, ka miratuar me Urdhër Nr.55, datë 31.07.2018, Udhëzimin "Për Metodologjinë e Organizimit dhe Funksionimit të CSIRT-eve në Nivel Kombëtar".

Sipas vetë deklarimeve të bëra nga infrastrukturat kritike dhe të rëndësishme të informacionit, ka një rritje të vogël përsa i përket pozicioneve të dedikuara të punës për sigurinë kibernetike për secilin sektor, duke treguar një përpjekje për të rritur kapacitetet njerëzore për mbrojtjen ndaj sulmeve kibernetike.

Gjithashtu, AKCESK në bashkëpunim dhe me partnerët, ka ndërmarrë një seri iniciativash trajnuese shumë të rëndësishme për të forcuar kapacitetet në fushën e sigurisë kibernetike. Këto trajnime, janë konceptuar dhe strukturuar për të adresuar sfidat në sigurinë kibernetike, të cilat variojnë nga mbrojtja e infrastrukturave kritike dhe të rëndësishme të informacionit, deri tek menaxhimi i incidenteve dhe analiza e kërcënimeve, dhe kanë si qëllim përmirësimin e njohurive dhe aftësive të profesionistëve në fushën e sigurisë kibernetike. Përmes këtyre programeve, të mbështetura dhe nga ekspertiza e partnerëve, AKCESK synon të rrisë ndërgjegjësimin mbi rreziqet aktuale kibernetike si dhe të ndërtojë një qëndrueshmëri më të fortë ndaj sulmeve të mundshme. Këto përpjekje reflektojnë një angazhim të

qartë për ngritjen e standardeve të sigurisë kibernetike dhe zhvillimit profesional, duke i përgatitur ata për të përballuar me efikasitet sulmet e mundshme kibernetike.

Kategoria e trajnimeve	Numri
Qeverisja (*Governance*)	25
Mbrojtja (*Defensive*)	42
Sulmi (*Offensive*)	2

Tabela 2. Trajnimet e OIKI dhe OIRI mundësuar nga partnerët e AKCESK

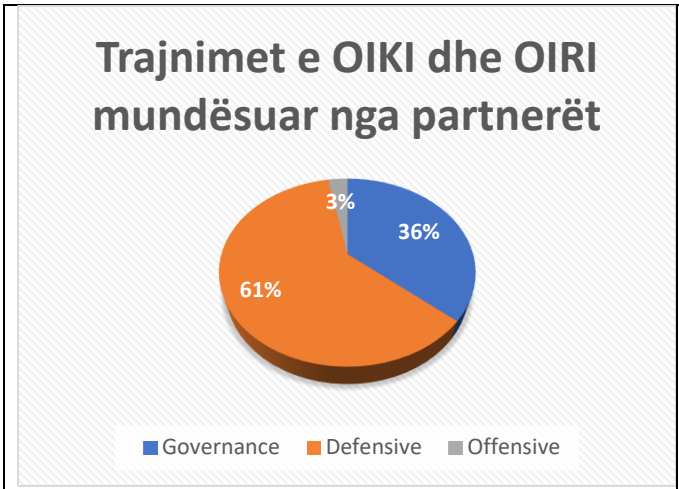


Figura 1. Trajnimet e OIKI dhe OIRI mundësuar nga partnerët e AKCESK

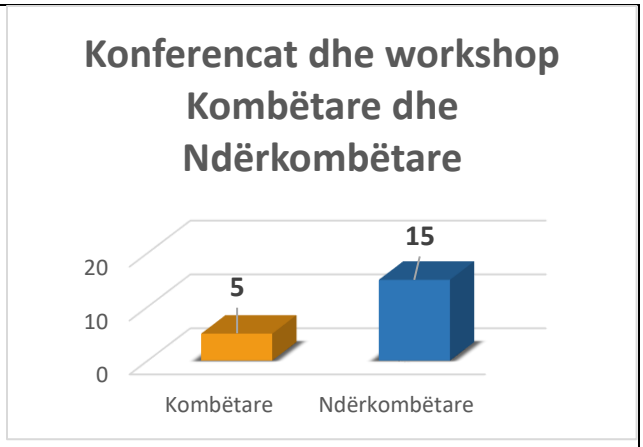


Figura 2. Konferencat dhe workshop-et Kombëtare dhe Ndërkombëtare

Gjatë vitit 2023, AKCESK ka organizuar trajnime dhe workshop-e për Operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit sipas sektorëve me qëllim prezantimin e Politikave dhe Masave të Sigurisë që çdo operator duhet të implementojë, si dhe përmirësimin e reagimit ndaj incidenteve kibernetike duke zhvilluar Table Top Exercises (TTX), Capture the Flag (CTF), si dhe simulime reale Cyber Drill.

Figura 3. Trajnimet e organizuara nga AKCESK

1. ZHVILLIMI I TEKNOLOGJISË DHE INFRASTRUKTURËS

Teknologjitë në fushën e sigurisë kibernetike janë të ndryshme dhe vazhdimisht po zhvillohen për të përballuar kërcënimet e shtuara në mjedisin kibernetik. Duke u nisur nga situata e sigurisë kibernetike në vend, AKCESK ka miratuar disa masa teknike kryesore (Baseline) të cilat duhet të implementohen nga të gjithë infrastrukturat kritike dhe të rëndësishme të informacionit në vend, të cilat përfshijnë:

- Të instalohen pajisje të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et).
- Të merren parasysh skemat "High-Availability" në pajisjet "core-network" në nivel perimetri (firewall), në nivel rutimi (L3) dhe komutimi paketash (L2) dhe nivel linjash fizike (L1).
- Të merren masa për shfrytëzimin e teknikave të pasqyrimit të dhënave (RAID 1/5/6/10) për të shmangur humbjen e të dhënave sensitive.
- Të merren masa për shmangien e "Single Point of Failure" tek shërbimet tuaja kritike dhe të rëndësishme.
- Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).
- Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).
- Të kryhen analiza të trafikut në nivel sjellje "behaviour" për pajisjet fundore.
- Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".
- Të implementohet sistem i automatizuar për menaxhimin dhe filtrimin e log-eve me qëllim identifikimin e alerteve në kohë reale.
- Nëse keni një departament zhvillimi, të realizohen testime të zhvillimeve të software-ve (stage-ing) në ambient të izoluar të ndarë nga ambienti i prodhimit(production).
- Të merren masa për implementim e një sistemi që kontrollon parametrat e sigurisë së një sistemi fundor, duke mos e lejuar këtë të fundit të jetë pjesë e rrjetit tuaj nëse këto parametra janë nën nivelin "Baseline" të dhënë më parë nga ju? (Sistem i cili kontrollon mungesën e patch-eve, update-t të Anti-Virusit etj.).
- Të izolohen logjikisht, (në VLAN-e të ndryshëm) Database dhe Web service-t (nëse janë të hostuara në ambientin tuaj).
- Të merren masa për ngritjen e DNS_SEC për të shmangur DNS Amplification attack dhe DNS_Poisoning attack.
- Të implementohet dhe testohet Disaster Recovery Site për shërbimet më të rëndësishme dhe kritike.
- Të merren masa për zëvendësimin ose izolimin e sistemeve "End of Life" të instaluara në pajisjet tuaja.
- Të merren masa për identifikimin dhe menaxhimin efektiv të aseteve dhe të realizohet vlerësimi i risqeve duke evidentuar:
    - Vjetërsisë
    - Afektimin e C/I/A (Konfidencialitetit/Integritetit/Disponueshmërisë
    - Vulnerabilitetet e identifikuara (CVE)
- Të hartohen plane dhe procedura të detajuara për menaxhimin e incidenteve kibernetike.
- Të merren masa për izolimin e rrjetit wireless nga pjesa tjetër e rrjetit.

- Të realizohen fushata ndërgjegjësimi të punonjësve në lidhje me sigurinë kibernetike dhe sulmet më të shpeshta si Phishing etj.
- Të kryhen testime për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (penetration test) dhe të hartohet plani për trajtimin e problematikave të evidentuara.
- Të kryhen kontrolle/audite të brendshme ose nga palët e treta për sigurinë e informacionit në infrastrukturat tuaja.
- Të kontrollohet nëse sistemi i Email-it nuk ka te konfiguruar featurat anti-spoofing: DMARC/SPF/DKIM.
- Të kontrollohen nëse ka Web Service që operon në protokollin http.
- Të kontrollohen nëse në firewall ka të ngritur White List të adresave të lejuara IP.
- Të përdoret politika e password-eve rastësore për userat/administratoret local (P.sh si LAPS të Microsoft).
- Të përdoret platforma Data Leakage Prevention për parandalimin e rrjedhjes së informacionit.
- Të përdoret teknika e mbrojtjes ndaj DoS/DDoS attack.
- Të përdoret teknika e Port Security te Switch-et ku numri maksimal i MAC Adresave të jetë 1 për përdoruesit e thjeshtë dhe një numër i limituar për ekspertët e IT-se ose Sigurisë Kibernetike.

Këto janë vetëm disa nga masat kryesore në fushën e sigurisë kibernetike, dhe është e rëndësishme për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit t'i plotësojnë me rigorozitet këto masa teknike si dhe të ndjekin zhvillimet më të fundit për të mbrojtur sistemet dhe rrjetet e tyre të informacionit nga kërcënime të ndryshme kibernetike.

AKCESK, bazuar në Baseline e masave të sigurisë kibernetike, kontrolleve të ushtruara, si dhe ndjekjen (*follow up*) të infrastrukturave kritike dhe të rëndësishme, ka realizuar vlerësimin e implementimit të tyre në nivel infrastrukture, si dhe në nivel sektorial.

Më poshtë paraqitet në mënyrë të përmbledhur niveli i implementimit të masave teknike të sigurisë nga infrastrukturat kritike dhe të rëndësishme të informacionit në nivel sektori.

Gjithashtu, në kuadër të mirëqeverisjes të sigurisë kibernetike u realizuan në bashkëpunim me infrastrukturat kritike dhe të rëndësishme të informacionit, analiza mbi buxhetet e dedikuara për sigurinë kibernetike për vitin 2023 dhe vitin 2024, si dhe investimet në sigurinë kibernetike për vitin 2023.

Nga të dhënat e mbledhura nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit rezulton se buxheti, si dhe planifikimi për projektet e fushës së sigurisë kibernetike ka një rritje të ndjeshme ndër vite, duke vënë në dukje sensibilizimin e infrastrukturave për investime konkrete në fushën e sigurisë kibernetike.

Më poshtë paraqitet në mënyrë të përmbledhur në nivel sektori buxheti i dedikuar dhe investimet për sigurinë kibernetike.

2. MBIKËQYRJA E IMPLEMENTIMIT TË QEVERISJES SË SIGURISË KIBERNETIKE

Identifikimi i infrastrukturave kritike dhe të rëndësishme të informacionit

AKCESK ka miratuar "Metodologjinë për identifikimin dhe klasifikimin e infrastrukturave kritike dhe infrastrukturave të rëndësishme të informacionit" (transpozuar nga Udhëzimet e ENISA-s dhe praktikat më të mira të BE-së). Lista e infrastrukturave kritike dhe të rëndësishme përditësohet të paktën një herë në dy vjet.
Faktorët që u aplikuan në identifikimin e infrastrukturave kritike dhe të rëndësishme janë:

a. **Efekti financiar** - ndikimi financiar që shkaktohet kur infrastruktura është jashtë funksionit.
b. **Shpërndarja gjeografike** - numri i individëve që mund të ndikohen nga mos marrja e shërbimit për shkak të mosfunksionimit të infrastrukturës.
c. **Efekti kohë** - përcakton intervalin në kohë, kur një shërbim nuk mund të ofrohet pasi infrastruktura është jashtë funksionit.

Sektorët e identifikuar si sektorë kritikë janë:

- Sektori Energjetik
- Sektori i Transportit
- Sektori Bankar
- Sektori Financiar
- Sektori Shëndetësor
- Sektori i Infrastrukturave digjitale
- Sektori i Furnizimit me ujë

Aktualisht, AKCESK është në proces të hartimit dhe miratimit të metodologjisë së re për identifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit.

Më poshtë gjeni numrin e infrastrukturave kritike dhe të rëndësishme të informacionit të identifikuara ndër vite.

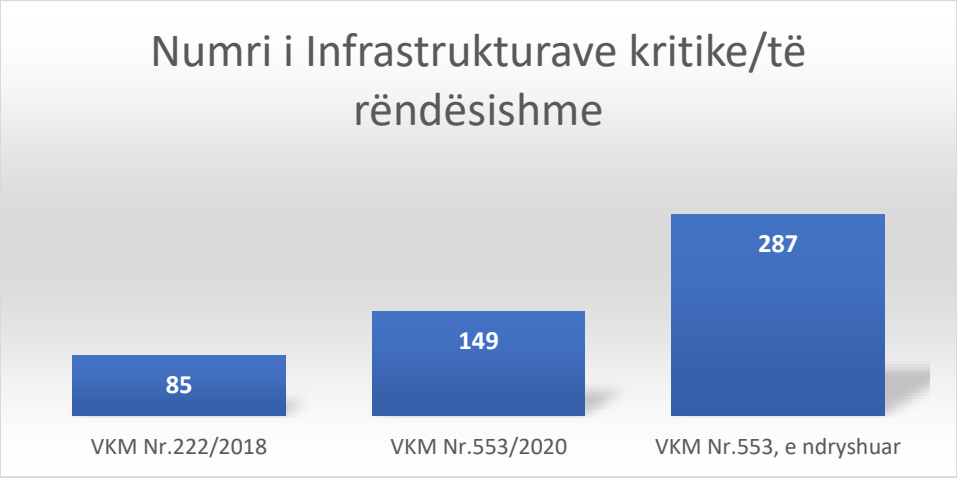


Figura 11: Infrastrukturat kritike dhe të rëndësishme të informacionit të identifikuara ndër vite.

Bazuar në VKM Nr. 553 datë 15.07.2020, e ndryshuar, janë identifikuar 145 Operatorë të Infrastrukturave Kritike dhe të Rëndësishme të Informacionit (14 prej të cilëve janë dhe kritike dhe të rëndësishme), të cilët administrojnë **287** sisteme dhe **41** rrjete për ofrimin e shërbimeve.

Figura 12. Operatorët e Infrastrukturave, sistemet dhe rrjetet sipas VKM Nr. Nr. 553/2020, e ndryshuar.

Në kuadër të punës së vazhdueshme për përmirësimin e procesit të identifikimit dhe klasifikimit të infrastrukturave të informacionit në përputhje me udhëzimet dhe standardet më të reja të BE-së, AKCESK ka punuar për rishikimin dhe hartimin e metodologjisë së re për identifikimin dhe klasifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe vijon angazhimin e vazhdueshëm për identifikimin e infrastrukturave të reja.

Menaxhimi i incidenteve kibernetike, si dhe analizimi i dobësive të konstatuara në fushën e sigurisë kibernetike

Përgjatë vitit 2023, AKCESK ka konstatuar shpeshtësinë dhe kategorinë e incidenteve të raportuara sipas sektorëve përkatës. Incidentet më të shpeshta janë raportuar nga sektori Bankar në masën 36% të totalit të incidenteve të raportuara duke e bërë atë si sektorin më të prekur nga incidente dhe sulme të mundshme kibernetike, më pas vjen me 31% të incidenteve të raportuara nga sektori i Infrastrukturave Digjitale, 12% sektori Energjetik, 7% sektori i Transportit, 7% sektori Financiar, 5% sektori Shëndetësor, si dhe 2% sektori i Telekomunikacionit.

Sektori	Nr. Incidenteve
Bankar	15
Infrastruktura digjitale	13
Energjetik	5
Transporti	3
Financiar	3
Shëndetësor	2
Telekomunikacion	1

Tabela 11. Numri i incidenteve të raportuara sipas sektorëve

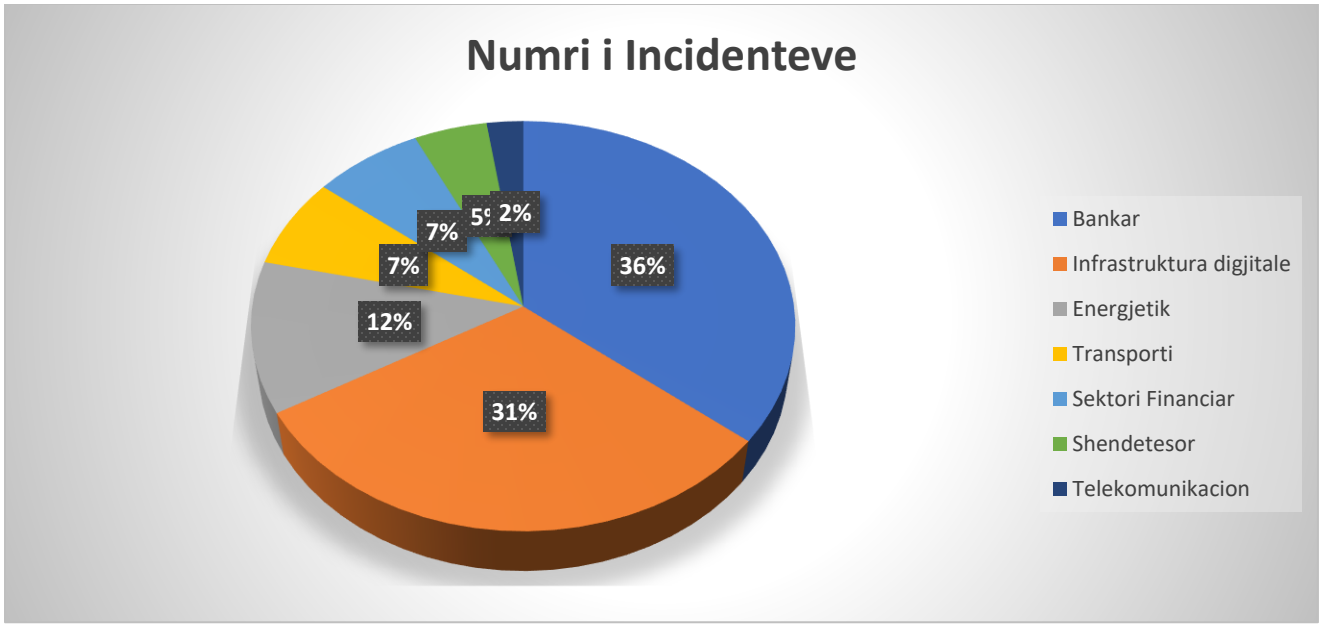


Figura 13. Numri i incidenteve të raportuara sipas sektorëve

Kategoritë e sulmeve të raportuara në nivel sektorial paraqiten si më poshtë:

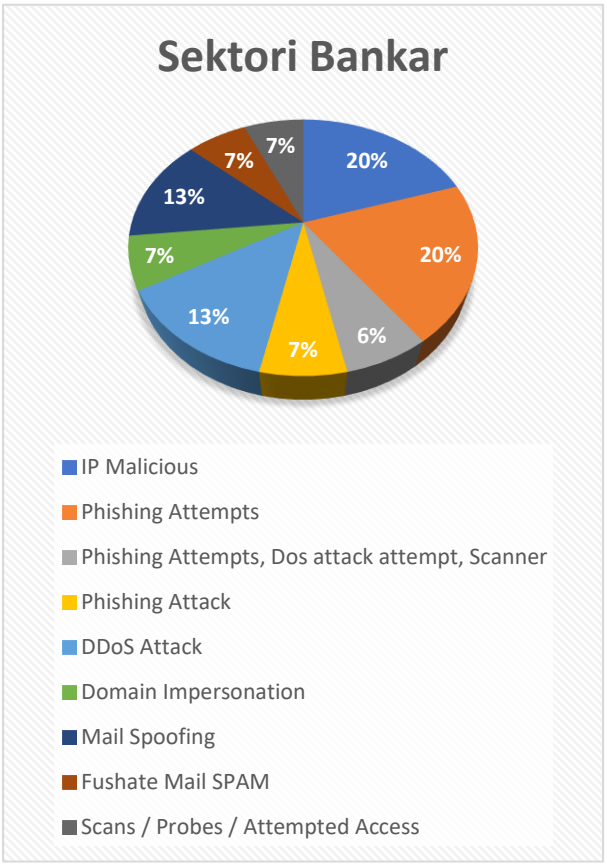


Figura 14. Kategoritë e incidenteve të raportuara në sektorin bankar

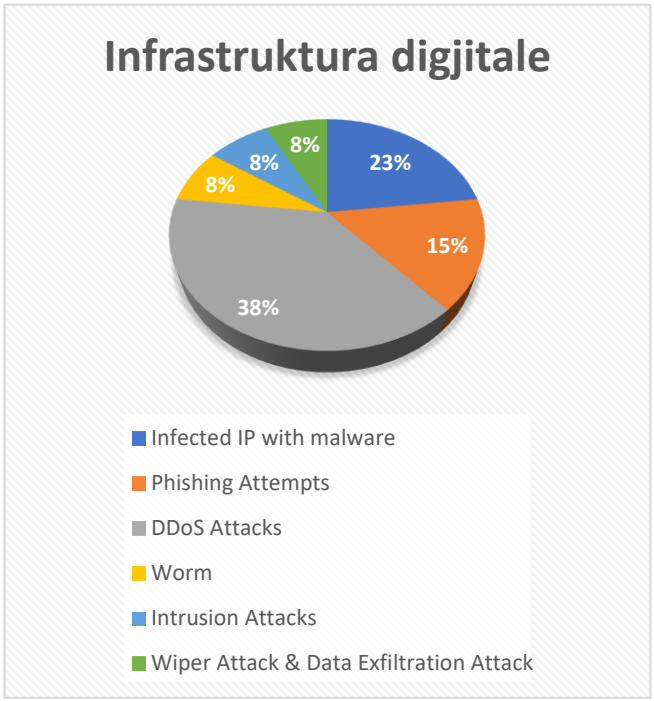


Figura 15. Kategoritë e incidenteve të raportuara në infrastrukturën digjitale

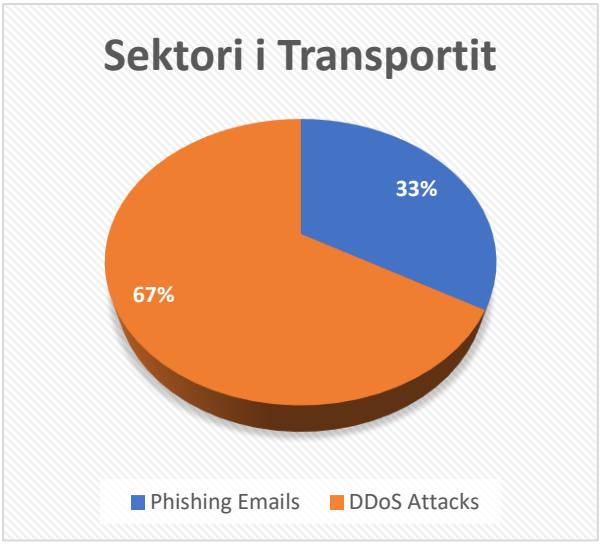


Figura 17. Kategoritë e incidenteve të raportuara në sektorin e transportit

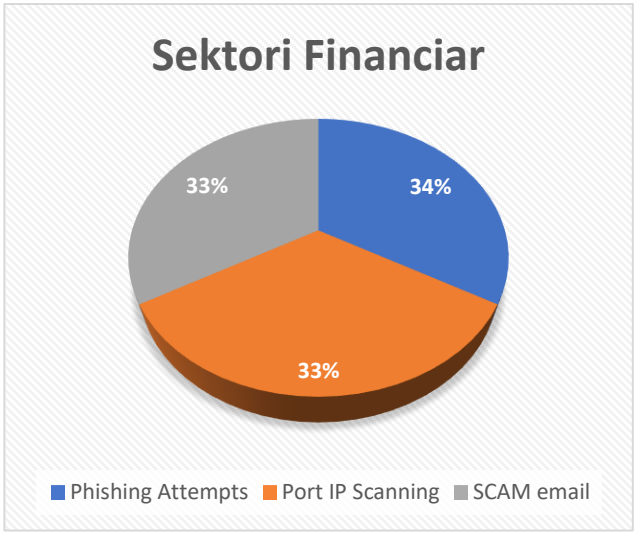


Figura 18. Kategoritë e incidenteve të raportuara në sektorin financiar

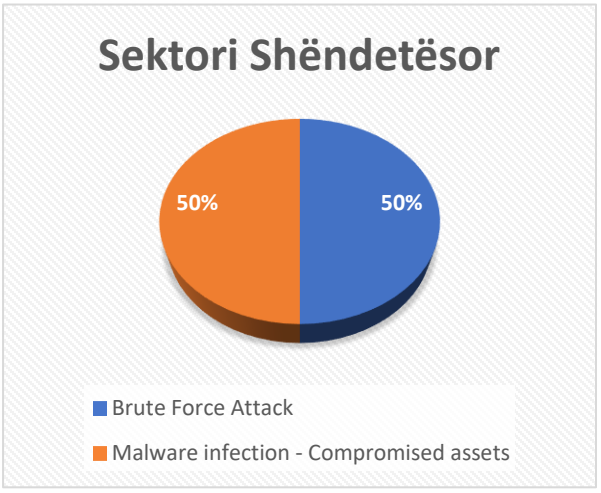


Figura 19. Kategoritë e incidenteve të raportuara në sektorin shëndetësor

Figura 20. Kategoritë e incidenteve të raportuara në sektorin e telekomunikacionit

Analiza e incidenteve kibernetike për vitin 2023 tregon një pamje të ndryshme të sigurisë kibernetike në sektorët kritikë. Këto incidente reflektojnë sfidat dhe tendencat aktuale në fushën e sigurisë kibernetike, si dhe ofrojnë një bazë për zhvillime strategjike të përmirësimit të sigurisë.

Numri i lartë i incidenteve në *sektorin bankar* tregon se infrastrukturat kritike dhe të rëndësishme të këtij sektori janë objektiv i lartë për sulmet kibernetike. Aktorët keqdashës janë të interesuar për vjedhjen e informacioneve sensitive, mohim të shërbimeve, prishjen e imazhit, destabilitet ekonomik. Gjatë vitit 2023 është vërejtur një rritje e konsiderueshme e tentativave phishing drejt sektorit bankar. Prandaj, një fokus i veçantë i duhet dhënë hartimit dhe zbatimit të politikave të sigurisë, monitorimit të vazhdueshëm të sistemeve kritike të informacionit, si dhe zbatimit të rekomandimeve të dhëna nga AKCESK.

Incidentet në infrastrukturat digjitale veçanërisht ato incidente të sponsorizuara nga shtete si Irani, Rusia të cilat përfshijnë tentativat për të ndërprerë shërbimet, vjedhjen e të dhënave sensitive, destabilitet ekonomik dhe politik, kërkojnë një përgjigje të koordinuar. Në këtë kontekst, bashkëpunimi ndërinstitucional dhe përdorimi i teknologjive të avancuara bëhen thelbësore për të ruajtur sigurinë kombëtare dhe integritetin e informacionit qeveritar.

Në *sektorin energjetik*, numri i incidenteve tregon një rrezik të konsiderueshëm ndaj infrastrukturës, duke theksuar nevojën për një përqendrim të madh në sigurinë e rrjeteve dhe sistemeve të ndërtuara mbi teknologji të lidhura me internetin.

Në *sektorin e transportit* incidentet shkaktohen nga tentativa për të ndërprerë shërbimin në sistemet kritike dhe të rëndësishme të informacionit. Këto përpjekje për ndërprerjet e shërbimeve në sistemet TIK, sinjalizojnë një nevojë kritike për përmirësimin e sigurisë së TI. Ky sektor kyç kërkon vëmendje të vazhdueshme për të parandaluar ndërhyrje të dëmshme.

Incidentet në *sektorin shëndetësor* theksojnë rëndësinë e sigurisë së të dhënave të pacientëve dhe funksionimin pa ndërprerje të sistemeve mjekësore. Përforcimi i sigurisë dhe mbrojtja e infrastrukturës kritike janë esenciale për integritetin e të dhënave të pacientëve.

Përgjithësisht, incidentet në sektorët e ndryshëm tregojnë një nevojë të shtuar për forcimin e sigurisë kibernetike në sistemet kritike apo të rëndësishme. Për të adresuar këtë sfidë, theksohet rëndësia e investimeve në trajnimin e stafit, përmirësimin e infrastrukturave të sigurisë, dhe monitorimin proaktiv të rreziqeve kibernetike. Këto veprime janë kyçe për të ngritur nivelin e mbrojtjes kibernetike në sektorë të ndryshëm, duke garantuar një mjedis më të sigurt në nivel kombëtar dhe ndërkombëtar

Rritja e ndjeshme e sulmeve kibernetike në gjysmën e dytë të 2021 dhe 2022 ka shënuar një kthesë në luftën kibernetike, veçanërisht ndikuar nga kriza Rusi-Ukrainë. Kjo periudhë ka rritur ndërgjegjësimin për rolin dhe ndikimin e luftës kibernetike në konfliktet globale, duke theksuar nevojën për rishikimin e normave ndërkombëtare në hapësirën kibernetike dhe adresimin e sfidave që vijnë nga sponsorizimi shtetëror i sulmeve kibernetike dhe shënjestrimi i infrastrukturave kritike civile.

Dinamika gjeo-politike e vendit tonë, e bën Shqipërinë një vend atraktiv për sulme të sofistikuara kibernetike.

Bashkëpunimet ndërkombëtare në fushën e sigurisë kibernetike janë esenciale për Shqipërinë, veçanërisht përmes iniciativave të NATO-s dhe BE-së. Këto bashkëpunime sigurojnë qasje në resurse dhe njohuri për të përballuar kërcënimet kibernetike përmes ndarjes së praktikave më të mira. Për më tepër është theksuar, roli i qeverisë dhe i sektorit privat në ndërtimin e një infrastrukture të informacionit të sigurt duke u fokusuar në rëndësinë e përgatitjes së burimeve njerëzore dhe teknologjike.

Sfidat e ardhshme për trajtimin e këtyre rreziqeve përfshijnë nevojat për të forcuar bashkëpunimin rajonal dhe global, investimet në teknologji të reja, përditësimin e legjislacionit për të pasqyruar ndryshimet në fushën e sigurisë kibernetike duke u siguruar të vihen në pah ndërveprimet gjeopolitike dhe vendimet politike që kanë një ndikim të drejtpërdrejtë në sigurinë kibernetike të një shteti.

Kërcënimet e vitit 2023 në Ballkanin Perëndimor u karakterizuan nga grupet kryesore të sulmuesve *"Advanced persistent Threat" (APT)* te lidhura me shtetin e Iranit si edhe grupe me origjine nga Rusia. Sulmet e tyre kryesore kanë qenë *ransomware* (lloj software i dëmshëm që bllokon qasjen në sistemin e kompjuterit ose të dhënat e përdoruesit deri në pagimin e një shpërblimi), *malware* (çdo software i dëmshëm që infekton ose dëmton një kompjuter ose rrjet), *inxhinieri sociale* (manipulimin e individëve për të fituar qasje në informacione të ndjeshme), *wiper* (lloj malware që synon të fshijë të dhënat e një sistemi, duke shkatërruar të dhënat e përdoruesit pa mundësi për rimëkëmbje). Tendencat në grupeve të sponsorizuara nga shteti përfshijnë shfrytëzimin e dobësive të njohura, targetimin e individëve, pajisjeve dhe aplikacioneve legjitime, si dhe ndërprerjen e shërbimeve publike dhe infrastrukturave kritike të informacionit.

AKCESK ka realizuar monitorim të vazhdueshëm të rrjeteve dhe sistemeve të informacionit, duke dërguar njoftime paralajmëruese dhe kundërmasa rast pas rasti, dhe duke koordinuar me operatorin, me qëllim rritjen e nivelit të sigurisë në nivel kombëtar. Shfrytëzimi i platformave monitoruese drejt një sërë rrjetesh dhe sistemesh të infrastrukturave të informacionit në Shqipëri 24 x 7 është një dëshmi e angazhimit të AKCESK për të siguruar një mjedis më të sigurt kibernetik.

Për të përballuar sfidat dhe rreziqet në fushën e sigurisë kibernetike, AKCESK ka theksuar rëndësinë e investimeve në trajnimin e stafit, përmirësimin e infrastrukturave të sigurisë së informacionit, dhe monitorimin proaktiv të rreziqeve kibernetike. Këto veprime janë kyçe për të ngritur nivelin e mbrojtjes kibernetike në sektorë të ndryshëm.

Roli i AKCESK në monitorimin, ndjekjen dhe rekomandimin e praktikave më të mira në menaxhimin e incidenteve kibernetike gjatë vitit 2023 ka qenë thelbësor për të adresuar sfidat dhe rreziqet në sigurinë kibernetike në Shqipëri.

Vlerësimi i sigurisë kibernetike në nivel sektorial

AKCESK, ka realizuar një vlerësim të nivelit të sigurisë të sektorëve kritikë, e cila bazohet në 3 komponentët e mëposhtëm:

- Komponenti i rrezikut të sistemeve të kompromentuar,
- Komponenti i diligjencës,
- Komponenti i sjelljes së përdoruesve (user behavior).

Këto tre shtylla janë analizuar për çdo infrastrukturë dhe më pas është realizuar mesatarizimi i tyre për të përcaktuar nivelin e sigurisë, ku vlerësimi i lartë tregon një nivel të lartë të sigurisë dhe një rrezik më të ulët kibernetik, ndërsa vlerësimi i ulët tregon rrezik të lartë. Mesatarizimi në nivel sektori ndihmon në vlerësimin e përgjithshëm të sigurisë.

Analiza e të dhënave në lidhje me vlerësimin e nivelit të sigurisë paraqet një përmirësim të qëndrueshëm në të gjithë sektorët kritikë. Rritja e nivelit të sigurisë rezulton nga implementimi i masave korrigjuese të sigurisë të evidentuara në raportet e kontrollit, rritjes së kapaciteteve njerëzore përmes trajnimeve të specializuara dhe rritjes së ndërgjegjësimit mbi çështjet e sigurisë, si dhe përmirësimit të kapaciteteve teknologjike dhe sistemeve të sigurisë. Këto masa kanë kontribuar në një rritje të nivelit të përgjithshëm të sigurisë në të gjithë sektorët kritikë, duke dëshmuar rëndësinë e një qasjeje gjithëpërfshirëse dhe të vazhdueshme ndaj menaxhimit të rreziqeve dhe përmirësimit të sigurisë.

3. PËRCAKTIMI I MASAVE TË SIGURISË KIBERNETIKE, SI DHE KONTROLLI I ZBATIMIT TË IMPLEMENTIMIT TË TYRE

Rregullorja "**Mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë** *(V. 2.0, miratuar me Urdhrin Nr. 10/2022)*" përcakton masat e sigurisë që duhet të implementojnë operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

AKCESK, kryen kontrolle të vazhdueshme të sigurisë kibernetike pranë infrastrukturave kritike dhe të rëndësishme të informacionit, për të mbikëqyrur përmbushjen e masave të sigurisë, nëpërmjet metodës se vetë deklarimit dhe vajtjes për kontroll në vend (Onsite). Përgjatë vitit 2023 u **katërfishua** numri i kontrolleve me vajtje në vend, në infrastrukturat kritike dhe të rëndësishme të informacionit. Kjo tregon fokusin e lartë që ka AKCESK për implementimin e masave të sigurisë nga infrastrukturat kritike dhe të rëndësishme të informacionit.

Më poshtë paraqiten në mënyrë të përmbledhur kontrollet e sigurisë kibernetike të realizuara nga AKCESK, për vitin 2023.

	Kontrolluar	Vetëdeklarim
Operatorët e Infrastrukturave Kritike të Informacionit	26	32
Operatorët e Infrastrukturave të Rëndësishme të Informacionit	23	22
Totali i Operatorëve të Infrastrukturave	49	54

Tabela 12. Kontrollet e sigurisë kibernetike

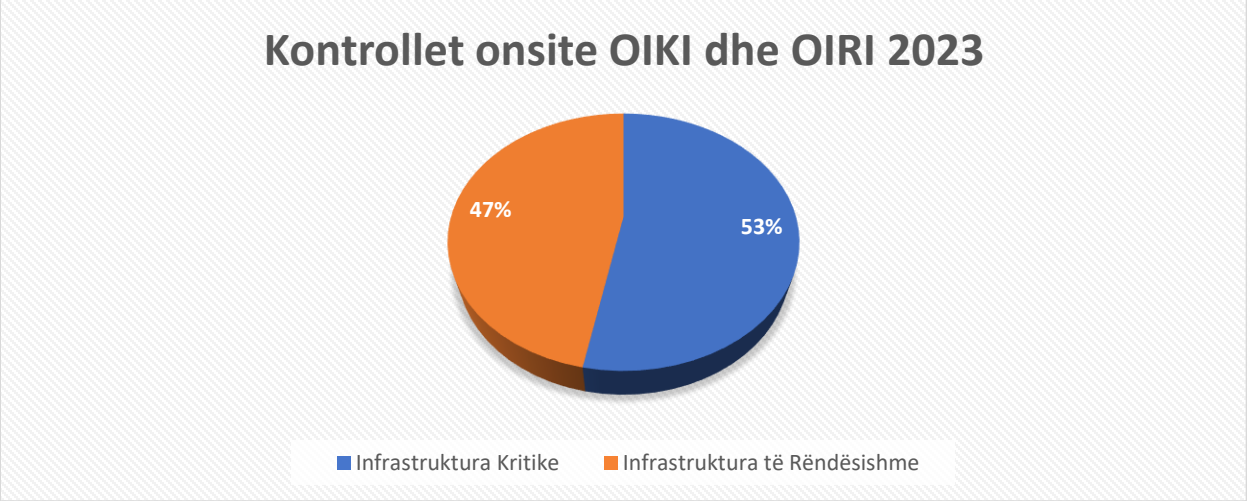


Figura 24. Kontrollet me vajtje në vend për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

Vlerësimi i vulnerabiliteteve (Vulnerability Assessment) nëpërmjet skanimeve aktive mbi operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit

AKCESK, përpara nisjes së procesit të kontrollit pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, kryen paraprakisht një vlerësim të vulnerabiliteteve të mundshme për adresat IP të vendosura në dispozicion nga vetë infrastrukturat e informacionit.

AKCESK, përdor burime të ndryshme të skanimit të cilat ndihmojnë në identifikimin dhe trajtimin e problematikave.

AKCESK, për vitin 2023 ka kryer në total ***27 Vlerësime të Vulnerabiliteteve (Vulnerability Assessment)*** për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit të përcaktuara në VKM Nr. 553, datë 15.7.2020 "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", e ndryshuar.

Pas realizimit të procesit të vlerësimit të vulnerabiliteteve, hartohet raporti me gjetjet përkatëse e cila përfshin:

1. Rezultatet e procesit të skanimit për IP e vendosura në dispozicion si dhe kohëzgjatja e këtij procesi.
2. Vlerësimi i nivelit te riskut që mund të kenë impakt në sistemet kritike apo te rëndësishme të informacionit:
    - Niveli i riskut Info **(0)**
    - Niveli i riskut i Ulët **(0.1 – 3.9)**
    - Niveli i riskut i Mesëm **(4.0 – 6.9)**
    - Niveli i riskut i Lartë **(7.0 – 8.9)**
    - Niveli i riskut Kritik **(9.0 – 10.0)**

3. Për vulnerabilitetet e identifikuara përcaktohet niveli i riskut, përshkrimi i vulnerabiliteteve dhe mënyra se si mund të kryhet mitigimi i tyre.

4. Rekomandimet e bazuara në gjetjet e procesit të skanimit. Këto rezultate nuk mund të konsiderohen si një matje përfundimtare e sigurisë për infrastrukturat kritike dhe të rëndësishme. Marrja në konsideratë e zgjidhjeve të propozuara në procesin e mitigimit ndihmojnë në uljen e nivelit të rrezikut për infrastrukturën. AKCESK, rekomandon të aplikohen të gjitha përditësimet e nevojshme bazuar në seksionin e procesit të mitigimit në secilin prej vulnerabiliteteve të shpjeguara më lart dhe gjithashtu të merren në konsideratë rekomandimet për të gjitha gjetjet shtesë.

Me qëllim minimizimin e rrezikut nga sulmet e mundshme kibernetike, AKCESK ka dhënë rekomandime për zëvendësimin e pajisjeve dhe sistemeve End of Life (EOL), si dhe të kryhen azhurnime periodike te software dhe sistemeve.

4. PROMOVIMI I NJË KULTURE KIBERNETIKE TË QËNDRUESHME /BURIMET NJERËZORE DHE NDËRGJEGJËSIMI

Promovimi i një kulture kibernetike të qëndrueshme është një proces afatgjatë dhe kërkon angazhim të vazhdueshëm për të ndërgjegjësuar shoqërinë mbi rreziqet e sigurisë kibernetike, si dhe përpjekje për të përmirësuar mbrojtjen duke zhvilluar dhe ngritur kapacitetet e nevojshme njerëzore në fushën e sigurisë.

AKCESK ka zbatuar programe trajnimi dhe ndërgjegjësimi në fushën e sigurisë kibernetike për të edukuar fëmijët, të rinjtë, prindër e mësues si dhe punonjësit socialë mbi rreziqet që mund të hasen në botën digjitale, metodat e mbrojtjes si dhe institucionet ku mund të raportohen rastet e kërcënimeve kibernetike.

Gjithashtu, AKCESK shpërndan materiale edukative, si dhe njoftime/lajme ditore mbi kërcënimet e mundshme kibernetike, incidentet kibernetike (të tilla si buletinet) në faqen zyrtare të Autoritetit[1], si dhe në rrjetet sociale.

AKCESK ka realizuar fushata ndërgjegjësuese dhe trajnime për ngritjen e kapaciteteve profesionale në fushën e sigurisë kibernetike, me OIKI dhe OIRI të tilla si stërvitje tavoline, seminare, dhe stërvitje kibernetike.

Ngritja e kapaciteteve njerëzore në fushën e sigurisë kibernetike është një element kyç i Strategjisë Kombëtare të Sigurisë Kibernetike dhe Planit të Veprimit 2020-2025.

AKCESK u ka dhënë prioritet trajnimeve dhe përgatitjes së ekspertëve në këtë fushë, me qëllim përmirësimin e aftësisë për të parandaluar, zbuluar dhe trajtuar sulmet kibernetike.

Konkretisht, gjatë vitit 2023 janë organizuar trajnime për ekspertët e institucioneve të sigurisë dhe mbrojtjes, si dhe OIKI dhe OIRI me tema:

- CompTIA Security+,
- Certified Information Systems Security Professional (CISSP),
- Certified Information Security Manager (CISM),
- SIM 3 Auditor Training,
- Risk Assessment Training,
- Hacker Fundamentals,
- Secure Coding,
- Industrial Control Systems (ICS) Live training,
- Industrial Control Systems (ICS) Cybersecurity Evaluation (401),
- Threat hunting,
- ISO 27001.

Gjithashtu, AKCESK në bashkëpunim me International Telecommunication Union, në kuadër të pilotimit të Projektit Global të ITU, "Creating a Safe and Prosperous Cyberspace for Children", kanë organizuar fushata ndërgjegjësimi për të edukuar, fuqizuar dhe këshilluar fëmijët, punonjësit për mbrojtjen e fëmijëve dhe prindërit, lidhur me kërcënimet me të cilat mund të përballen në internet. AKCESK në bashkëpunim dhe me Agjencinë Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës (ASHDMF), ka realizuar disa trajnime me temë "Mbrojtja e fëmijëve në internet dhe higjiena kibernetike", ku janë trajnuar punonjësit e Njësive për Mbrojtjen e Fëmijëve në bashki të ndryshme të vendit. Krahasuar me vitet e mëparshme, numri i trajnimeve ka ardhur në rritje dhe temat kanë qenë gjithnjë e më të avancuara, në përputhje me zhvillimet e fundit në sigurinë kibernetike.

5. BASHKËPUNIMI KOMBËTAR DHE NDËRKOMBËTAR

Rreziqet kibernetike janë të pamundura për t'u adresuar në mënyrë efikase vetëm nga një institucion apo një vend i vetëm. Prandaj, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike bashkëpunon me institucione publike dhe private në nivel kombëtar me qëllim parandalimin, trajtimin

[1] Faqe zyrtare e AKCESK: www.cesk.gov.al

dhe mbrojtjen sa i përket kërcënimeve kibernetike. Gjithashtu, qeveria shqiptare ka bashkëpunuar me organizata ndërkombëtare si dhe me institucione të tjera homologe, për të ndarë informacion, përvoja, si dhe për të adresuar rreziqet kibernetike.

Bashkëpunimi kombëtar

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në rolin e institucionit koordinator në fushën e sigurisë kibernetike në vend, ka nënshkruar Marrëveshje Mirëkuptimi për bashkëpunim të mëtejshëm në fushën e sigurisë kibernetike me institucione dhe operatorë të infrastrukturave si:

- Shoqata Shqiptare e Bankave (2023),
- Akademinë e Forcave të Armatosura (2023),
- Kuvendin e Republikës së Shqipërisë (2023),
- Postën Shqiptare (2023),
- Operatorin e Shpërndarjes së Energjisë Elektrike (2023),
- Operatorin e Sistemit të Transmetimit (2023),
- Bankën e Parë të Investimeve (2023),
- Union Bank (2023),
- Raiffeisen Bank (2023),
- Tirana Bank (2023),
- Risi Albania Project (2023),
- Policia e Shtetit,
- Autoriteti i Mediave Audiovizive dhe Qendra e Koordinimit Kundër Ekstremizmit të Dhunshëm (2021),
- Autoriteti i Komunikimeve Elektronike dhe Postare (2019),
- Akademia e Studimeve Politike (2019).

Bashkëpunimi Ndërkombëtar

Bashkëpunimi me NATO-n dhe **OSBE-në:** Shqipëria është anëtare e NATO-s dhe OSBE-së dhe është e përfshirë në aktivitetet dhe programet e tyre për sigurinë kibernetike. Ky bashkëpunim ka përmirësuar ndarjen e informacionit, shkëmbimin e përvojave dhe ngritjen e kapaciteteve në fushën e sigurisë kibernetike në rajon dhe më gjerë.

Bashkëpunimi me Bashkimin Evropian: Shqipëria në kuadër të anëtarësimit në Bashkimin Evropian është e angazhuar në harmonizimin e legjislacionit vendas me direktivat, rregulloret dhe standardet e BE-së në fushën e sigurisë kibernetike.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka nënshkruar Marrëveshje Mirëkuptimi për shkëmbim informacioni në fushën e sigurisë kibernetike me:

- Emiratet e Bashkuara Arabe (2023),
- Izraelin (2023),

- 4IG (2023),
- Rumaninë (CERT-RO),
- Maqedoninë e Veriut (MKD-CIRT),
- Kosovën (KOS-CERT).

Gjithashtu, Shqipëria është anëtare e forumeve ndërkombëtare si ITU, FIRST, FESA, TF-CSIRT, TRUSTED INDRODUCER dhe CRI.

AKCESK gjithashtu ka vijuar komunikimin me agjenci të ndryshme të sigurisë kibernetike të vendeve anëtare të BE-së me qëllim vendosjen dhe forcimin e bashkëpunimit në fushën e sigurisë kibernetike për arritjen e objektivave të përbashkëta dhe standardeve evropiane sa i përket sigurisë kibernetike.

Bashkëpunimi ndërkombëtar në fushën e sigurisë kibernetike është i rëndësishëm, për të adresuar sfidat e shtuara të kësaj fushe. Shqipëria është e përfshirë aktivisht në këtë proces dhe punon bashkë me partnerët ndërkombëtarë për të forcuar sigurinë kibernetike dhe për të përmirësuar kapacitetet e saj për të parandaluar dhe trajtuar sulmet kibernetike.

Diplomacia e Sigurisë Kibernetike

Republika e Shqipërisë si vend anëtar i OSBE, ka marrë angazhimin për implementimin e masave për ndërtimin e besimit (CBM 15) në fushën e sigurisë kibernetike me qëllim krijimin e një mjedisi të sigurt kibernetik nëpërmjet forcimit të bashkëpunimit.

Gjithashtu, në cilësinë e vendit anëtar në Kombet e Bashkuara (UN), Shqipëria ka rol dhe përgjegjësi në çështjet e sigurisë kibernetike në këtë organizatë ndërkombëtare. Republika e Shqipërisë ka të drejtë të ndërmarrë veprime dhe të luajë një rol aktiv në diplomacinë e sigurisë kibernetike në kuadër të OKB-së, NATO-s, OSBE-së dhe forumeve të tjera ndërkombëtare ku bën pjesë, dhe mbi të gjitha, në kuadër të interesave kombëtare në hapësirën kibernetike dhe objektivave të politikës së jashtme dhe politikave të sigurisë në nivel kombëtar.

Më datat 6 - 10 Mars 2023, AKCESK ishte pjesë e punimeve të sesionit të IV të "*Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies*" në Kombet e Bashkuara. Fokusi i këtij sesioni ishin kërcënimet globale të sigurisë kibernetike, masat e ndërtimit të besimit, ngritja e kapaciteteve, si dhe normat e sjelljes së përgjegjshme të shteteve në hapësirën kibernetike. Në deklaratën e Shqipërisë u theksua progresi në harmonizimin e kuadrit ligjor me kornizën e Bashkimit Evropian si dhe arritjet në lidhje me ngritjen e CSIRT Kombëtar; trajnimeve për rritje kapacitetesh të CSIRT-eve sektoriale; konsolidimin e kapaciteteve për diplomacinë kibernetike dhe qeverisjen kibernetike; trajnimeve dhe fushatave të ndërgjegjësimit për administratën publike, industrinë, fëmijët e të rinjtë; si dhe trajtimin e temave të sigurisë kibernetike në kurrikulat arsimore.

Politikat e sigurisë kibernetike janë të përshtatura me sfidat aktuale të sigurisë kibernetike duke pasur parasysh zhvillimet e shpejta në teknologji dhe rritjen e rreziqeve kibernetike. Synimi i këtyre politikave është arrija e një niveli të lartë të sigurisë kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellë ndërmjet subjekteve që operojnë në fushën e sigurisë kibernetike, për të promovuar një mjedis të sigurt për zhvillimin e ekonomisë dhe shoqërisë së informacionit në Shqipëri.

Në figurën e mëposhtme paraqiten në mënyrë grafike marrëveshjet e bashkëpunimit kombëtare dhe ndërkombëtare për vitin 2023:

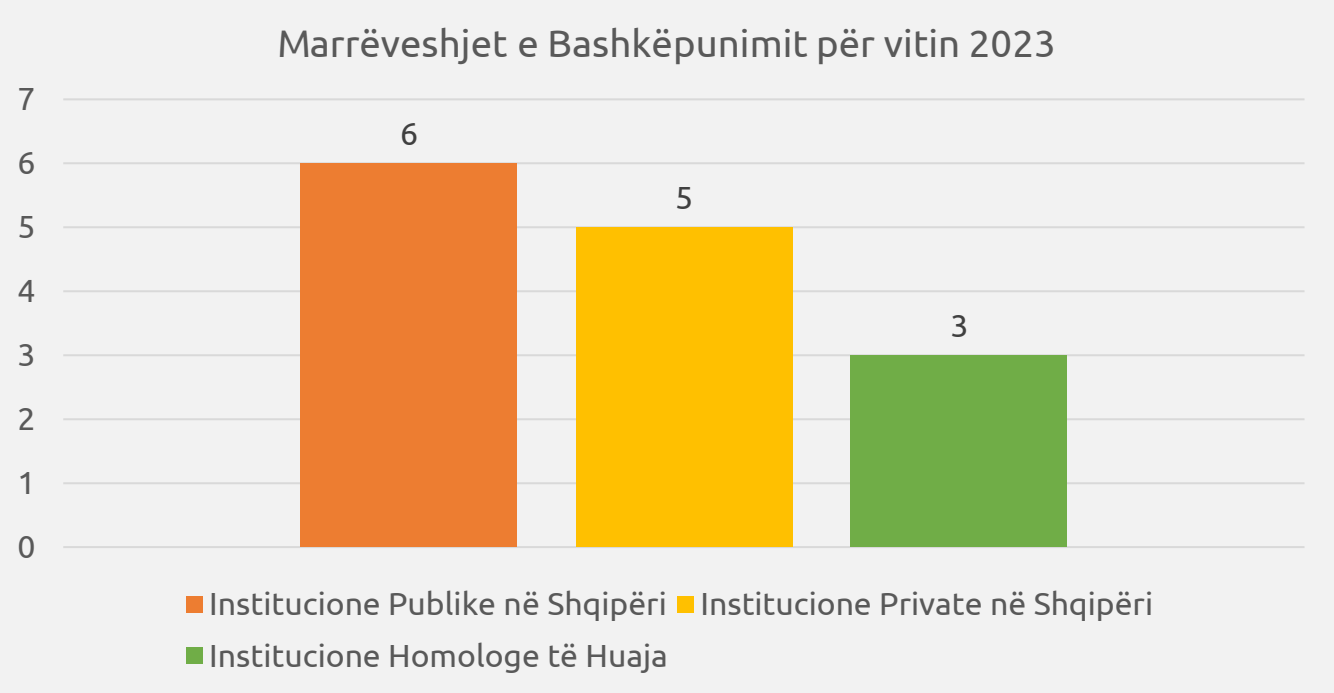


Figura 26. Marrëveshjet e bashkëpunimit për vitin 2023

V. RASTET E NJOHURA TË SULMEVE KIBERNETIKE

Rastet e Njohura: Një analizë e shkurtër e rasteve të njohura të sulmeve kibernetike të ndodhura në Shqipëri dhe ndikimi i tyre.

Deri në vitin 2021, Shqipëria nuk ishte target për sulmet kibernetike të mëdha dhe të njohura. Një nga sulmet kibernetike më të sofistikuar ndaj sistemeve qeveritare shqiptare, ishte ai i vitit 2022, me origjinë nga shteti Islamik i Iranit, ku qëllimi i keqdashësve ishte fshirja e gjithë sistemeve qeveritare dhe të dhënave të tyre. Menjëherë pas identifikimit të sulmit ransomware nisën bllokimet, në mënyrë që të mos përhapej më tej, dhe nga implementimi korrekt i politikave të backup-it dhe rikuperimit nga fatkeqësia, brenda javës së parë shërbimet u rikthyen në gjendje pune.

Megjithatë, ashtu si në shumë vende të tjera, aktualisht sulmet kibernetike janë bërë një rrezik potencial dhe ndikimi i tyre mund të prekë:

Infrastrukturat kritike dhe të rëndësishme të informacionit: Sulmet ndaj infrastrukturave kritike dhe të rëndësishme të informacionit mund të shkaktojnë ndërprerje të shërbimeve dhe ndikim serioz në ekonominë dhe stabilitetin e vendit. Sulmet e mundshme kibernetike mund të prekin:

1. **Sektorin energjetik:** Sulmet ndaj sistemeve të energjisë elektrike dhe gazit mund të shkaktojnë ndërprerje në furnizimin e energjisë elektrike dhe ngrohjes. Këto sulme mund të dëmtojnë infrastrukturën dhe të sjellin pasoja serioze në jetën e qytetarëve dhe aktivitetet ekonomike.

2. **Sektorin e Transportit:** Sulmet kibernetike kundër sistemeve të transportit mund të dëmtojnë infrastrukturën rrugore, ajrore, detare duke shkaktuar ndërprerje të trafikut dhe ndikime të mëdha në lëvizjen e njerëzve dhe mallrave.
3. **Sektorin Shëndetësor:** Sistemet në sektorin e shëndetësisë janë të rëndësishme për ruajtjen e të dhënave mjekësore dhe funksionimin e shërbimeve shëndetësore. Sulmet ndaj tyre mund të dëmtojnë të dhënat mjekësore, qasjen e mjekëve në informacionin e pacientëve, si dhe shërbimet mjekësore në përgjithësi.
4. **Sektorin Bankar/Financiar:** Institucionet bankare/mikrofinanciare janë shpesh target për sulmet kibernetike, për vjedhjen e të dhënave të kartave të kreditit, vjedhjen e llogarive bankare, dhe kërcënimet ransomware. Këto sulme mund të dëmtojnë klientët, të shkaktojnë humbje të mëdha financiare, si dhe humbje të reputacionit.
5. **Sektorin e infrastrukturave digjitale:** Sulmet kibernetike kundër institucioneve qeveritare mund të kenë ndikime serioze. Nëse një sulm kibernetik ka sukses, ai mund të kompromet ojë të dhënat sensitive dhe informacionin e ndjeshëm të qeverisë, duke përfshirë të dhënat e qytetarëve.

Individët dhe bizneset: Sulmet kibernetike ndaj individëve dhe bizneseve janë të zakonshme. Kjo përfshin tentativat për vjedhjen e të dhënave personale, apo sulmet ransomware që mund të bllokojnë qasjen në të dhënat. Disa lloje të zakonshme të sulmeve kibernetike të hasura në Shqipëri ndaj individëve dhe bizneseve përfshijnë:

- **Phishing,**
- **Ransomware,**
- **Malware,**
- **Social engineering.**

Përgatitja e Shqipërisë ndaj sulmeve kibernetike

Shqipëria ka ndërmarrë hapa për të parandaluar sulmet kibernetike duke ngritur kapacitetet njerëzore në fushën e sigurinë kibernetike, si dhe duke promovuar ndërgjegjësimin rreth rreziqeve të mundshme kibernetike.

Për të mbrojtur infrastrukturat kritike dhe të rëndësishme të informacionit, AKCESK ka përcaktuar masat e sigurisë kibernetike te cilat duhen të implementohen nga OIKI dhe OIRI, si dhe kryen kontrolle periodike për të verifikuar implementimin e tyre.

Gjithashtu, AKCESK kryen monitorim të vazhdueshëm të sigurisë të OIKI dhe OIRI, duke kryer testime të vulnerabiliteteve për të parandaluar dhe zbuluar sulmet potenciale. Bashkëpunimi ndërkombëtar në këtë aspekt është i rëndësishëm për të adresuar kërcënimet kibernetike të përbashkëta.

Për të mbrojtur biznesin nga sulmet kibernetike, AKCESK ka hartuar manuale, udhëzime mbi praktikat më të mira të sigurisë kibernetike ku përfshihet përdorimi i fjalëkalimeve komplekse, azhurnimi i programeve dhe sistemeve kompjuterike, ndërgjegjësimi i punonjësve mbi rreziqet e mundshme

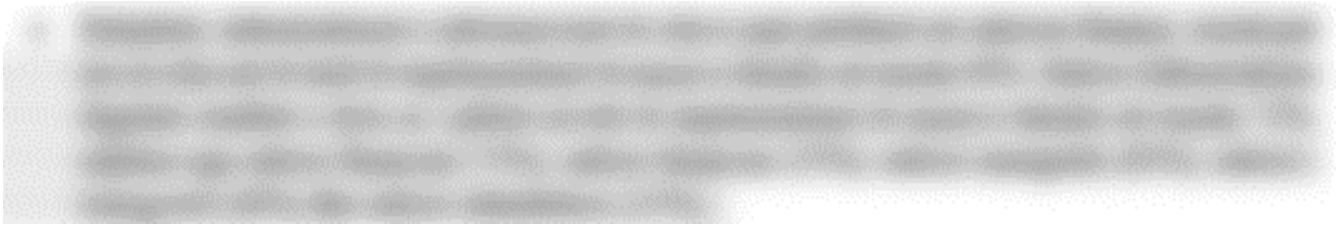
kibernetike. Gjithashtu, AKCESK vazhdimisht rekomandon bizneset mbi hartimin e një plani për menaxhimin e incidenteve kibernetike në rast se ndodh një sulm kibernetik.

VI. VLERËSIMI I PËRGJITHSHËM: KONKLUZIONE DHE REKOMANDIMET

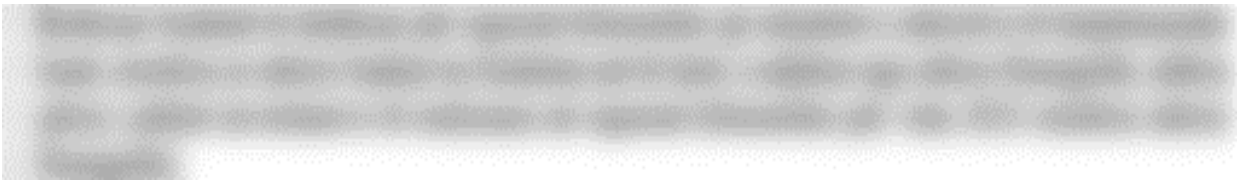
KONKLUZIONE

Siguria kibernetike është një sfidë e madhe në epokën digjitale dhe ka një rëndësi të jashtëzakonshme për të ardhmen, jo vetëm në Shqipëri, por edhe në nivel ndërkombëtar. Nga analiza e aspekteve të qeverisjes së sigurisë kibernetike, arrihet në disa konkluzione si vijon:

- Shqipëria ka bërë progres sa i përket politikave strategjike, duke hartuar politika në përputhje me standardet e BE-së dhe duke përditësuar në vazhdimësi ato ekzistuese si Plani i Veprimit i Strategjisë Kombëtare për Sigurinë Kibernetike i cili është rishikuar për të adresuar sfidat dhe prioritetet aktuale të sigurisë kibernetike në nivel kombëtar.
- Sa i përket legjislacionit, Shqipëria ka miratuar ligjin e ri në përputhje me Direktivën e BE-së NIS 2 dhe po punon për hartimin e akteve nënligjore në zbatim të tij.
- Nga analiza e qeverisjes së sigurisë kibernetike sipas sektorëve, arrihet në përfundimin se sektorët duhet t'i japin më shumë prioritet sigurisë kibernetike në terma të rritjes së kapaciteteve njerëzore dhe teknike për të mbuluar nevojat që mund të shfaqen nga kërcënimet kibernetike.
- Nga analiza e numrit të pozicioneve të dedikuara për sigurinë kibernetike për sektorin bankar, energjetik, financiar, shëndetësor dhe të transportit, nga të dhënat aktuale, vihet re se pritet të ketë rritje të lehtë të stafit të sigurisë kibernetike për vitin 2024.
- Për sa i përket zhvillimit të teknologjisë dhe infrastrukturës në sektorët kritikë, AKCESK ka përcaktuar disa masa teknike të sigurisë kibernetike, të cilat përfshijnë edhe implementimin e zgjidhjeve të ndryshme teknologjike me qëllim rritjen e sigurisë kibernetike.



- Për të pasur një qeverisje të sigurisë kibernetike efektive, planifikimi buxhetor dhe implementimi i projekteve të dedikuara në fushën e sigurisë kibernetike kanë një rol kyç.



- AKCESK ka punuar për identifikimin dhe klasifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit në mënyrë të vazhdueshme, ku nga 85 infrastruktura kritike dhe të rëndësishme që ishin në vitin 2018, me VKM Nr. 553, datë 15.07.2020, të ndryshuar, numri shkoi në 287, dhe aktualisht vijon procesi për miratimin e Projektvendimit të ri që do ta rrisë numrin e infrastrukturave të informacionit të identifikuara dhe klasifikuara.

- Me qëllim rritjen e sigurisë së infrastrukturave kritike dhe të rëndësishme të informacionit, Shqipëria ka identifikuar "Crown jewels", që mund të jenë të ekspozuara ndaj sulmeve kibernetike, përfshirë sektorin energjetik, transportit, bankar, financiar, shëndetësor, infrastruktura digjitale, dhe furnizimi me ujë. Identifikimi i tyre mundëson që të forcohen më tej masat e sigurisë kibernetike përkatëse për funksionimin e qëndrueshëm të këtyre sistemeve.
- Shqipëria ka ndërmarrë hapa për t'u mbrojtur dhe përgatitur për përgjigje ndaj sulmeve kibernetike duke ngritur kapacitetet teknike dhe njerëzore në fushën e sigurisë kibernetike, si dhe duke promovuar ndërgjegjësimin rreth rreziqeve të mundshme kibernetike.
- Aktivitetet me qëllim rritjen e kapaciteteve si dhe fushatat e ndërgjegjësimit kanë pësuar rritje duke ndikuar në përmirësimin e aftësive teknike të ekspertëve të sigurisë kibernetike të institucioneve publike si dhe të gjithë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, dhe duke kontribuar në rritjen e ndërgjegjësimit të gjithë shoqërisë mbi rreziqet kibernetike dhe masat parandaluese.

Shqipëria ka bërë hapa pozitive në fushën e sigurisë kibernetike, por ende ka sfida të mëdha përpara. Për të përmbushur synimin e rritjes së nivelit të sigurisë kibernetike në vend, rëndësi të veçantë i duhet dhënë përmirësimit të kapaciteteve njerëzore në këtë fushë, investimit në teknologjinë dhe infrastrukturën e nevojshme në fushën e sigurisë kibernetike, rritjes së bashkëpunimit me sektorin privat dhe organizatat ndërkombëtare.

Nga ky raport mund të evidentohen disa pika të forta dhe pika të dobëta të cilat janë shpjeguar në vijim:

Pikat e forta

- **Plotësimi i kuadrit ligjor, strategjia, dhe politikat në fushën e sigurisë kibernetike:** Shqipëria ka plotësuar kuadrin e nevojshëm ligjor, ka të miratuar strategjinë kombëtare për sigurinë kibernetike, si dhe ka zhvilluar politika të rëndësishme në fushën e sigurisë kibernetike konform direktivave dhe praktikave më të mira të BE-së. Kjo është një pikë e fortë për të përgatitur më mirë vendin dhe koordinuar përpjekjet në këtë fushë.
- **Krijimi dhe forcimi i kapaciteteve të Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike:** Ky është një hap i rëndësishëm për të koordinuar efektivisht punën për

rritjen e sigurisë kibernetike përmes krijimit, forcimit dhe zbatimit të politikave dhe masave të sigurisë kibernetike në nivel kombëtar, si dhe për të ndihmuar në parandalimin e sulmeve kibernetike dhe reagimin e shpejtë ndaj incidenteve.

- **Rritja e nivelit të "Implementimi i masave të sigurisë kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit",** sipas rekomandimeve dhe masave të lëna nga kontrollet e kryera nga ACESK në sektorë ndryshëm gjatë vitit 2023.
- **Krijimi i Qendrës Kombëtare Operacionale të Sigurisë (SOC)** që shërben për trajtimin e incidenteve kibernetike, si dhe ofron ndihmë në zbulimin e burimit të sulmeve.
- **Bashkëpunimi ndërkombëtar:** Shqipëria është e përfshirë në bashkëpunim ndërkombëtar në fushën e sigurisë kibernetike me organizata dhe forume të ndryshme ndërkombëtare si: NATO, OSBE, OKB, ITU, FIRST, FESA, TF-CSIRT, TRUSTED INDRODUCER, CRI, si në të ardhmen synon të krijojë anëtarësime dhe bashkëpunime të reja.

Pikat e dobëta / Dobësitë

- **Investimet në fushën e sigurisë tek infrastrukturat kritike dhe të rëndësishme të informacionit**: Megjithëse gjatë vitit të fundit janë bërë përpjekje për të përmirësuar sigurinë në rrjetet dhe sistemet e informacionit, ende ka nevojë për investime të mëtejshme për të siguruar një infrastrukturë më të fortë dhe më të sigurt.

[redacted]

REKOMANDIME

Nga analiza e mësipërme, dalin rekomandimet për veprime të mundshme për të përmirësuar qeverisjen kibernetike në Shqipëri si vijon:

- **Legjislacioni dhe Politikat:** Hartimi i kuadrit nënligjor në zbatim ligjit të ri, duke përfshirë të gjithë elementët të cilët mungojnë në legjislacionin ekzistues. Ky opsion do të garantonte bazën e duhur ligjore në fushën e sigurisë kibernetike, duke vendosur rregulla të qarta për të gjithë subjektet e përfshira.
- **Miratimi i Planit të Veprimit të përditësuar të Strategjisë Kombëtare të Sigurisë Kibernetike**: Qeveria duhet të shqyrtojë dhe të miratojë Planin e Veprimit të rishikuar për periudhën 2024-2025 në përputhje me zhvillimet më të reja në këtë fushë.
- **Investime në teknologji në fushën e sigurisë kibernetike** për të përmirësuar sigurinë dhe qëndrueshmërinë e sistemeve kritike

[redacted]

- **Bashkëpunimi me sektorin privat**: Autoriteti duhet të punojë për të ndërtuar marrëdhënie të ngushta me sektorin privat. Bashkëpunimi do të ndihmojë në ndarjen e informacionit mbi kërcënime kibernetike dhe në koordinimin e masave të sigurisë.

- **Bashkëpunimi Ndërkombëtar**: Duhet të rritet niveli i bashkëpunimit me organizata të shoqërisë civile dhe partnerë ndërkombëtarë për të përmbushur objektivat e sigurisë kibernetike
- **Edukimi dhe trajnimi në fushën e sigurisë kibernetike**: I gjithë personeli i administratës publike duhet të marrë trajnime të rregullta në sigurinë kibernetike. Gjithashtu, duhet të promovohet ndërgjegjësimi i përdoruesve të rrjetit.
- **Mbrojtja e fëmijëve në internet**: Mbrojtja e fëmijëve në mjedisin online, përmes programeve të ndërgjegjësimit dhe bashkëpunimit me organizata dhe partnerë që kanë për qëllim sigurinë e fëmijëve në internet.
- **Stimulimi i investimeve**: Inkurajimi i investimeve në teknologji të avancuara dhe inovacion në sigurinë kibernetike për të forcuar mbrojtjen dhe për të parandaluar sulmet kibernetike.
- **Monitorimi i përdorimit të teknologjive të reja**: Monitorimi i përdorimit të teknologjive të reja, si inteligjenca artificiale dhe *machine learning,* për të siguruar që ato të përdoren në mënyrë të sigurtë dhe të përputhen me rregullat dhe standardet e sigurisë kibernetike.
- **Rritja e ndërgjegjësimit në fushën e IoT:** Ngritja e ndërgjegjësimit për rreziqet e sigurisë në internet të gjërave (IoT) dhe përparësitë e sigurisë kibernetike në këtë fushë, duke ofruar trajnime dhe edukim për profesionistët dhe përdoruesit.
- **Forcimi i CSIRT-eve**: Forcimi dhe përmirësimi i qendrave të përgjigjes për incidente kibernetike (CSIRT) në nivel kombëtar për të siguruar reagim efektiv në rast të incidenteve kibernetike
- **Monitorimi i rëndësishëm i rrjeteve**: Përmirësimi i monitorimit të rrjeteve dhe sistemeve për të zbuluar dhe parandaluar sulmet kibernetike në kohë dhe për të minimizuar dëmin e mundshëm.
- **Rritja e Besimit dhe Transparencës**: Rritja e transparencës dhe llogaridhënies në fushën e sigurisë kibernetike për të ndërtuar besim në publik dhe në sektorin privat.