RAPORT VJETOR

2023

Rr. "Papa Gjon Pali II", Nr. 3, Kati I
Tiranë, Shqipëri

TABELA E PËRMBLEDHJES

MESAZH I DREJTORIT TË PËRGJITHSHËM

Të nderuar,

Është kënaqësi që t'ju prezantojmë Raportin Vjetor të vitit 2023 të Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK). Ky raport ofron një pasqyrë të detajuar të arritjeve dhe progresit tonë gjatë vitit në fushën e shërbimeve të besuara dhe sigurisë kibernetike në Shqipëri.

Misioni ynë është të arrijmë një nivel të lartë të sigurisë kibernetike, përmes përcaktimit të masave të sigurisë, detyrimeve dhe të drejtave, si dhe një bashkëpunimi të ngushtë ndërmjet të gjitha palëve që operojnë në këtë fushë. Ne jemi përkushtuar të garantojmë një nivel të lartë të besueshmërisë dhe sigurisë në shërbimet e besuara, transaksionet elektronike ndërmjet qytetarëve, bizneseve dhe autoriteteve publike, duke rritur efikasitetin e shërbimeve publike dhe private dhe të tregtisë elektronike, për të krijuar një mjedis të sigurt elektronik.

Në 2023, veprimtaria jonë u fokusua në disa drejtime kryesore: forcimi i kuadrit ligjor për sigurinë kibernetike, rishikimi i planit të veprimit të strategjisë kombëtare të sigurisë kibernetike, ngritja e kapaciteteve teknike për mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit, zgjerimi i bashkëpunimit ndërinstitucional, përmirësimi i përgjigjeve ndaj sulmeve kibernetike, si dhe zhvillimi i partneriteteve strategjike me organizata ndërkombëtare dhe qeveritare.

Gjatë këtij viti, Shqipëria përjetoi sulme të shumta kibernetike, që synonin institucione shtetërore dhe kompani private. AKCESK, në bashkëpunim me partnerët tanë, ka arritur të menaxhojë këto kërcënime me profesionalizëm të lartë, duke minimizuar dëmet dhe rikuperuar shërbimet e prekura.

Gjithashtu, kemi vazhduar punën për implementimin e Sistemit të Menaxhimit të Sigurisë së Informacionit në institucionin tonë, bazuar në standardet ndërkombëtare të sigurisë së informacionit. Ky implementim luan një rol të rëndësishëm në menaxhimin efikas të sigurisë së informacionit dhe ofron një garanci të fortë për trajtimin e duhur për të dhënat e infrastrukturave kritike dhe të rëndësishme të informacionit.

Ne mbetemi të përkushtuar ndaj vizionit tonë për të ndërtuar një mjedis të sigurt kibernetik në Shqipëri dhe për të garantuar besueshmërinë e shërbimeve tona për të gjithë qytetarët.

Me respekt,
Prof. Asoc. Dr. Igli Tafa

HYRJE

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (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 Ligjit Nr. 2/2017, "Për Sigurinë Kibernetike" dhe akteve nënligjore të nxjerra në zbatim të tyre.

QËLLIMI I RAPORTIT

Ky dokument është Raportim mbi veprimtarinë e Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, për periudhën Janar – Dhjetor 2023.

Qëllimi i këtij Raporti Vjetor është:

- Të prezantojë progresin e veprimtarisë së Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.
- Të analizojë prioritetet kryesore të Autoritetit.
- Të identifikojë çështje, apo sfida për të ardhmen e punës së Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.
- Të sigurojë transparencë në veprimtarinë e Autoritetit.

Raporti vjetor ndihmon në transmetimin e informacionit për të interesuarit, përfshirë mbështetësit, donatorët, autoritetet, dhe publikun në përgjithësi.

Raporti shërben si një mjet për të vlerësuar dhe përmirësuar veprimtarinë e institucionit në të ardhmen.

I. AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

AKCESK 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 Ligjit Nr. 2/2017, "Për Sigurinë Kibernetike" dhe të akteve nënligjore të nxjerra në zbatim të tyre.

MISIONI

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.
Garanton sigurinë për shërbimet e besuara, në veçanti për garantimin e besueshmërisë dhe sigurisë në transaksionet elektronike ndërmjet qytetarëve, biznesit dhe autoriteteve publike, duke rritur efektivitetin e shërbimeve publike e private dhe tregtisë elektronike, si dhe përcakton standardet minimale teknike për sigurinë e të dhënave dhe rrjeteve/sistemeve të informacionit, në përputhje me standardet ndërkombëtare në këtë fushë, me qëllim krijimin e një mjedisi të sigurt elektronik.

SYNIMI

Krijimi i një institucioni që nëpërmjet zbatimit të ligjit dhe standardeve teknike ndërkombëtare me tolerancë zero, krijon besueshmëri për përdoruesit e nënshkrimit elektronik, identifikimit elektronik, shërbimeve të besuara si dhe rrit sigurinë në rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë.

FUNKSIONET E AKCESK

1. Regjistron/ akrediton Ofruesin e Shërbimit të Besuar dhe mbikëqyr veprimtarinë e tij.
2. Inspekton metodat e gjenerimit dhe menaxhimit të çelësave publik, dhe certifikatave elektronike.
3. Mbikëqyr procesin e lëshimit të certifikatave të kualifikuara elektronike dhe implementimin e nënshkrimit elektronik, identifikimin elektronik dhe shërbimet e tjera të besuara.
4. Garanton standardet mbi identifikimin e sigurt të individëve, të cilëve iu lëshohen certifikatat e kualifikuara elektronike.
5. Përcakton masat e Sigurisë Kibernetike në nivel Kombëtar.
6. Pikë qendrore kontakti në nivel kombëtar për operatorët përgjegjës në fushën e sigurisë kibernetike dhe bashkërendon punën për zgjidhjen e incidenteve të sigurisë kibernetike.
7. Vepron në cilësinë e CSIRT-së kombëtar.
8. Siguron ndihmë dhe mbështetje metodike për operatorët përgjegjës në fushën e sigurisë kibernetike.
9. Kryen aktivitete ndërgjegjësimi dhe edukimi në fushën e sigurisë kibernetike.
10. Autoriteti koordinon veprimtaritë e tij me institucionet e sigurisë dhe të mbrojtjes dhe bashkëpunon me CSIRT-të sektoriale dhe autoritetet ndërkombëtare në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi.

II. VEPRIMTARIA E AKCESK NË VITITN 2023

Në vitin 2023, Autoriteti fokusoi veprimtarinë e tij në fushat e mëposhtme:

1- Forcimin e kuadrit ligjor për sigurinë kibernetike, me qellim mbrojtjen e infrastrukturave kritike te informacionit dhe menaxhimin efektiv te incidenteve.
2- Zgjerimi i Marrëveshjeve të Bashkëpunimit dhe Mirëkuptimit me institucione bankare, shtetërore dhe me shtetin e Izraelit në përballimin e sfidave kibernetike.
3- Përgatitjen e rregulloreve dhe materialeve informueses në lidhje me Sigurinë Kibernetike
4- Kontrolli i infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me implementimin e masave të Sigurinë Kibernetike.
5- Ngritja e kapaciteteve për reagim ndaj sulmeve kibernetike dhe ndërtimi i një strukture të fortë të monitorimit për të parandaluar incidente të ngjashme në të ardhmen.
6- Ndërtimi i partneriteteve strategjike me organizata ndërkombëtare dhe qeveritare për të përforcuar bashkëpunimin dhe shmangur krizat kibernetike në nivel Kombëtar.
7- Zhvillimi i programeve të trajnimit dhe të ndërgjegjësimit për sigurinë kibernetike në publikun dhe sektorin privat, për të rritur vetëdijen dhe kapacitetet për mbrojtje.

8- Përpjekjet për rritjen e transparencës dhe llogaridhënies së AKCESK në veprimtarinë e tij, duke siguruar që të dhënat dhe raportet e tij të jenë të qasshme dhe të vërtetueshme nga publiku dhe institucionet e tjera.
9- Përdorimi i teknologjisë së avancuar dhe zhvillimi i mjeteve të avancuara për të zbuluar, monitoruar dhe parandaluar sulmet kibernetike në mënyrë efektive.

IMPLEMENTIMI I STANDARDEVE TË ORGANIZATËS NDËRKOMBËTARE PËR STANDARDIZIM (ISO 27001)

Gjatë vitit 2023, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka punuar për implementimin e Sistemit të Menaxhimit të Sigurisë së Informacionit në institucion bazuar në Standardin ISO 27001. Implementimi i këtij standardi është një proces që siguron një qasje të sigurt në menaxhimin e informacionit.

Implementimi i ISO 27001 do të ndihmojë Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike të sigurojë një nivel të lartë të sigurisë së informacionit dhe të përmbushë standardet ndërkombëtare në këtë fushë.

BASHKËPUNIMI DHE PARTNERËT

AKCESK ka nxitur bashkëpunimin me parterë të cilët kanë në fokus kryesor Sigurinë Kibernetike duke:

- Organizuar seminare për të ndarë eksperiencën dhe praktikat më të mira në fushën e sigurisë kibernetike.
- Krijuar programe të përbashkëta për trajnime dhe certifikime në sigurinë kibernetike për të rritur kapacitetet e punonjësve dhe partnerëve të tyre.
- Bashkëpunuar në hulumtime dhe zhvillime të përbashkëta teknologjike për të përmbushur objektivat e sigurisë kibernetike në nivel lokal dhe ndërkombëtar.

FORCIMI I KAPACITETEVE ADMINISTRATIVE

Bazuar në një përmbledhje të nevojave kryesore të identifikuara në vitin 2023, stafi i AKCESK ka ndjekur trajnime dhe certifikime në disa fusha, si më poshtë vijon:

- Cyber Crisis and Communication Workshop – 10 punonjës
- CompTIA Security + - 12 punonjës
- Senior Policymaker Cyber Strategy Planning Workshop – 3 punonjës
- CISSP Training – 10 punonjës
- Cybersecurity Risk Management and Baseline Security for Organizations – 2 punonjës
- Risk Assessment Training – 8 punonjës
- Hacker Fundamentals – 3 punonjës
- Secure Coding - 3 punonjës
- Threat Hunting Exercise – 10 punonjës
- Workshop on governing cyber crisis - 10 punonjës
- Cyber Defense Strategy Development – 4 punonjës
- Senior Policymaker Cyber Strategy Planning Workshop – 3 punonjës

- Cyber Security in Public Administration – 2 punonjës
- USTI Cybersecurity Policies and Strategy Training Sequence – 3 punonjës
- ICS Training – 2 punonjës
- Train the Trainers Course on Cyberhygiene – 2 punonjës
- Cyber Diplomacy and Policy Course - 2 punonjës
- Cyber security governance - 2 punonjës
- Zero Trust - 2 punonjës
- Defending against adversary actions – 1 punonjës
- Seasonal School on Digital Transformation 2023 – 2 punonjës
- WB3C Training for CISOs of Critical Infrastructure in WB – 1 punonjës

REZULTATET E PROJEKTEVE TË REALIZUARA

Gjatë vitit 2023 ACESK ka realizuar projekte në bashkëpunim me organizata kombëtare dhe ndërkombëtare si mëposhtme:

PROJEKTI

Një dekadë ndërgjegjësim për sigurinë online të fëmijëve – workshop për përmbylljen e një projekti dy-vjeçar.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), në bashkëpunim me Unionin Ndërkombëtar të Telekomunikacionit (International Telecommunication Union-ITU), zhvilloi një workshop më 6 dhjetor 2023, si pjesë e përmbylljes së një projekti dyvjeçar të nisur në shtator 2021. Qëllimi kryesor i këtij projekti ishte ndërgjegjësimi dhe bashkëpunimi mbi sigurinë e fëmijëve në internet, duke rritur kapacitetet dhe ndërgjegjësimin përmes trajnimeve dhe fushatave ndërgjegjësuese për fëmijët, të rinjtë, mësuesit, prindërit dhe punonjësit social. Workshop-i solli së bashku përfaqësues nga institucionet shtetërore, shoqëria civile, dhe sektori privat për të diskutuar mbi legjislacionin aktual, nevojat e reformave dhe për të theksuar rëndësinë e një hapësire më të sigurt kibernetike për fëmijët. Diskutimet përfshinë gjithashtu prezantimin e rezultateve të aktiviteteve të zhvilluara gjatë periudhës së projektit në të gjithë Shqipërinë.

REZULTATET E PROJEKTIT

Rezultatet e projektit janë si vijon:

- Tre video promovuese në gjuhën shqipe bazuar në Udhëzimet e ITU për mbrojtjen e fëmijëve në internet, shpërndarë në media kombëtare online, që synojnë të edukojnë fëmijët, të rinjtë, prindërit, mësuesit dhe operatorët e industrisë.
- Manual për fëmijët, i shpërndarë në 12 qarqe të Shqipërisë për ndërgjegjësimin e fëmijëve dhe të rinjve për rreziqet online.
- Përgatitja e manualit "Train the Trainer" për prindërit, mësuesit dhe kujdestarët për të forcuar mbrojtjen e fëmijëve në internet.
- Shpërndarja e një Mesazhi të Unifikuar me aktorët kryesorë të industrisë për të rritur sigurinë online për fëmijët.
- Hartimi i një Raporti të Ndikimit për të vlerësuar ndërgjegjësimin dhe të mësuarit para dhe pas trajnimeve.
- Organizimi i 12 seminareve online për fëmijët dhe të rinjtë me qëllim rritjen e ndërgjegjësimit dhe angazhimin e komuniteteve rinore në procesin e konsultimit mbi iniciativat e lidhura me mbrojtjen e fëmijëve në internet si dhe 15 seminareve për prindërit dhe mësuesit për të rritur aftësitë e tyre digjitale, në mënyrë që të jenë të aftë të mbrojnë fëmijët dhe të rinjtë në internet.
- Realizimi dhe shpërndarja e një broshure me këshilla për sigurinë në internet.
- Organizimi i 5 seminareve me palët e interesuara të industrisë për të rritur bashkëpunimin në mbrojtjen e fëmijëve në internet.
- Zhvillimi i 5 seminareve për profesionistët e TIK-ut dhe 12 aktiviteteve për ngritjen e kapaciteteve për mësuesit dhe ekspertët e qeverisë mbi aftësitë përkatëse të kërkuara për të forcuar sigurinë në internet për fëmijët në kontekstin e fushave të fokusit të ITU.
- Përgatitja e dy raporteve: Raporti për Vlerësimin e Përparësisë dhe Raporti për Planin e Zbatimit për Politikat e Mbrojtjes së Fëmijëve në Internet në Shqipëri.

AKTIVITETE KRYESORE GJATË VITIT 2023

Seminari 3-ditor "Senior Policymaker Cyber Strategy Planning"

Seminari 3-ditor "Senior Policymaker Cyber Strategy Planning", u organizua nga Autoriteti Kombëtar për CESK në bashkëpunim me Departamentin Amerikan të Shtetit dhe MITRE Corporation në datat 24-26 janar 2023.

Qëllimi i seminarit 3- ditor ishte finalizimi i zhvillimit të kornizave të një Strategjie Kombëtare për Sigurinë Kibernetike, e cila përfshin hartimin e qëllimeve të politikës, identifikimin e iniciativave mbështetëse për secilin qëllim, identifikimin e aktorëve për secilën iniciativë dhe rekomandimet për sfidat dhe tejkalimin e tyre për implementimin e aktiviteteve.

Seminari, nën drejtimin e MITRE Corporation, u fokusua në rolin e secilit institucion të sigurisë dhe të mbrojtjes në hartimin e strategjive të sigurisë dhe politikave për menaxhimin e çështjeve të sigurisë kibernetike, si dhe harmonizimin e planeve strategjike me praktikat më të mira të SHBA-ve.

Trajnimi CISSP

Në kuadër të planit të ri strategjik për forcimin e sigurisë kibernetike në nivel kombëtar, me mbështetjen e e-GA, gjatë vitit 2023 është iniciuar një seri trajnimesh, e dedikuar për rritjen e kapaciteteve profesionale të stafeve përgjegjës të sigurisë kibernetike në Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, si edhe në disa prej infrastrukturave kritike të informacionit në vend.

Në këtë kuadër, në datat 27 Shkurt – 3 Mars 2023, përfaqësues të AKCESK dhe përfaqësues të disa prej infrastrukturave kritike të informacionit kryen me sukses trajnimin CISSP.

Konferenca “Sfidat e Sigurisë Kibernetike në Shqipëri”

Në kuadër të Ditës Ndërkombëtare të Internetit të Sigurt Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) në bashkëpunim me Prezencën e OSBE-së në Shqipëri, USAID / DAI, Agjencinë Kombëtare të Shoqërisë së Informacionit (AKSHI), Shoqatën Shqiptare të Bankave, Soft&Solution, R&T Group, One Telecommunications dhe DigitALB organizuan konferencën “Sfidat e Sigurisë Kibernetike në Shqipëri”, pranë MAK Albania hotel më datë 07.02.2023.

Qëllimi i konferencës ishte rritja e nivelit të sigurisë kibernetike në vend në zbatim të Planit të ri Strategjik për sigurinë kibernetike, nëpërmjet adresimit të sfidave aktuale të sigurisë kibernetike, si dhe forcimi i bashkëpunimit me partnerët dhe bashkëpunëtorët strategjikë, duke konsideruar edhe kontributin e çmuar të ekspertëve të fushës nga diaspora. Pjesëmarrësit përfshinin përfaqësues të qeverisë, diplomatë, dhe liderë të industrisë që diskutuan mbi rritjen e ndërgjegjësimit dhe bashkëpunimin për të minimizuar dëmet nga sulmet kibernetike. Konferenca përfshiu gjithashtu sesione mbi mbrojtjen e infrastrukturave kritike dhe rëndësinë e gjithëpërfshirës për të rritur qëndrueshmërinë kibernetike.

Trajnimi: Rritja e Kapaciteteve Njerëzore në fushën e Sigurisë Kibernetike

Më datë 11.04.2023, në kuadër të planit të ri strategjik për forcimin e sigurisë kibernetike në nivel kombëtar, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, zhvilloi trajnimin e dedikuar për rritjen e kapaciteteve profesionale të stafeve përgjegjëse të sigurisë kibernetike të infrastrukturave kritike dhe të rëndësishme të informacionit në vend.

Trajnimi i organizuar përfshiu dy sesione paralele të dedikuara për forcimin e sigurisë kibernetike të infrastrukturave të informacionit. Në sesionin e parë, stafet e infrastrukturave të reja kritike dhe të rëndësishme, të identifikuara në 2022, u njohën me kuadrin ligjor aktual, rëndësinë e ngritjes së CSIRT-ve sektoriale, përgjegjësitë dhe proceset e identifikimit të infrastrukturave, si dhe me masat e sigurisë kibernetike që duhet të zbatohen. Sesioni i dytë përfshinte ushtrime praktike "Table Top Exercise" për përfaqësuesit e infrastrukturave ekzistuese, ku u diskutuan skenarë të ndryshëm për të forcuar ndërgjegjësimin, kapacitetet teknike dhe hartimin e procedurave të sigurisë për të menaxhuar dhe parandaluar incidentet kibernetike.

Nënshkrimi i Marrëveshjes së Bashkëpunimit në fushën e Sigurisë Kibernetike ndërmjet AKCESK dhe Emirateve të Bashkuara Arabe

Me datë 05.04.2023 u nënshkrua Marrëveshja e Bashkëpunimit në fushën e sigurisë kibernetike ndërmjet AKCESK dhe Emirateve të Bashkuara Arabe. Me nënshkrimin e kësaj Marrëveshje të rëndësishme, AKCESK filloi një kapitull të ri bashkëpunimi me partnerët strategjikë të Emirateve të Bashkuara Arabe, drejt sigurimit të kufijve të padukshëm të hapësirës kibernetike të Shqipërisë, nëpërmjet shkëmbimit të informacionit, shkëmbimit të praktikave më të mira dhe fuqizimit të kapaciteteve njerëzore.

Stërvitja rajonale e sigurisë kibernetike

Stërvitja kibernetike 4 ditore, e organizuar nga Akademia e Qeverisjes Elektronike të Estonisë (eGovernance Academy), CybExer Technologies, Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI), Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) dhe autoritetet e tjera kompetente të sigurisë, me mbështetjen e Bashkimit Evropian, u mbajt në Tiranë ku morën pjesë ekspertë të sigurisë kibernetike nga Shqipëria, Mali i Zi, dhe Maqedonia e Veriut. Ekipi shqiptar, i udhëhequr nga përfaqësues të AKSHI dhe AKCESK, me pjesëmarrës dhe nga institucionet e tjera të sigurisë dhe infrastrukturat kritike të informacionit, tregoi aftësi të shkëlqyera në kundërpërgjigjen ndaj një simulimi sulmi kibernetik duke u renditur në vendin e parë.

Aktiviteti u ndoq nga Presidenti i Republikës së Shqipërisë SH.T.Z. Bajram Begaj së bashku me Presidentin e Republikës së Estonisë, SH.T.Z. Alar Karis dhe Ambasadoren e Bashkimit Evropian SH.S.Znj. Christiane Hohmann.

TTX dhe Cyber Drill për sektorin e Transportit dhe Energjisë

Në datat 6-7 nëntor 2023, në bashkëpunim me Risi Albania u zhvillua trajnimi me temë "Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës" për sektorët e transportit dhe energjetikës. Gjatë këtij trajnimi dy ditor u bënë prezantime lidhur me kuadrin ligjor, strategjinë, politikat, masat e nevojshme të sigurisë që duhet të ndërmerren nga infrastrukturat e informacionit dhe nevojat për qeverisje kibernetike. Pjesë e rëndësishme e këtij trajnimi ishte gjithashtu zhvillimi i dy Table Top Exercises për menaxhimin e incidenteve dhe krizës kibernetike, kërcënime kibernetike industriale që përfshijnë sulme mbi sistemet IT, OT dhe IoT, si dhe simulimi i sulmit "Phishing", ku në skenarët e zhvilluar u analizuan raste nga infektimi me malware (programe keqdashëse). Gjithashtu u organizua Cyber Drill nëpërmjet platformës FISA.al, ku u zhvilluan ushtrime konkrete mbi identifikimin dhe menaxhimin e incidenteve kibernetike.

TTX dhe Cyber Drill për sektorin Financiar dhe Siguracionet

AKCESK, i fokusuar në rritjen e nivelit të sigurisë kibernetike në infrastrukturat e informacionit në nivel kombëtar, gjatë vitit 2023 ka mbështetur Operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit për rritjen e kapaciteteve profesionale dhe teknike.

Me mbështetjen e partnerit tonë Risi Albania/Helvetas dhe kontributin e ekspertëve të AKCESK, me 23-24 nëntor 2023 u zhvillua aktiviteti trajnues me sektorin financiar/bankar.

Aktiviteti dy ditor u përqendrua në zhvillimin e skenarëve të ndryshëm TTX, të dedikuar për këtë sektor dhe pjesëmarrësit u përfshinë në stërvitjen Cyber Drill, duke treguar aftësitë e tyre në zgjidhjen e incidenteve kibernetike mbështetur në procedurat përkatëse.

TTX dhe Cyber Drill për Institucionet e pavaruara, Sektorin e Ujit, AKSHI dhe Policia e Shtetit

Në vazhdim të objektivit së AKCESK për rritjen e kapaciteteve si një ndër shtyllat kryesore për mbrojtjen e infrastrukturave të informacionit me mbështetjen e partnerit tonë Risi Albania/Helvetas dhe kontributin e ekspertëve të Autoritetit, zhvilloi në datat 20, 21 dhe 22 Dhjetor 2023, trajnimin e parashikuar me temë "Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës" për Institucionet e Pavaruara, Sektorin UK, AKSHI dhe Policinë e Shtetit.

Për vetë rëndësinë që këta sektorë kanë përsa i përket infrastrukturave të informacionit që ata administrojnë, gjatë këtij trajnimi tre ditor u bënë prezantime lidhur me kuadrin ligjor, strategjinë, politikat, masat e nevojshme të sigurisë që duhet të ndërmerren nga infrastrukturat e informacionit dhe nevojat për qeverisje kibernetike.

Pjesë e rëndësishme e këtij trajnimi ishte zhvillimin i tre skenarëve të ndryshëm TTX, për menaxhimin e incidentit kibernetik. Gjithashtu u zhvilluan 2 ditë stërvitje kibernetike (Cyber Drill) me ushtrime konkrete mbi menaxhimin e incidentit kibernetik, nëpërmjet platformës FISA.al.

ARRËVESHJE BASHKËPUNIMI DHE MEMORANDUME 2023

- Marrëveshje Bashkëpunimi me Raiffeisen Bank.
- Marrëveshje Bashkëpunimi me Operatorin e Shpërndarjes së Energjisë Elektrike (OSHEE).
- Marrëveshje Bashkëpunimi me Union Bank.
- Marrëveshje Bashkëpunimi me Tirana Bank.
- Marrëveshje Bashkëpunimi me Bankën e Parë të Investimeve.
- Marrëveshje Bashkëpunimi me Kuvendin e Republikës së Shqipërisë.
- Marrëveshje Bashkëpunimi me Operatorin e Sistemit të Transmetimit (OST).
- Marrëveshje Bashkëpunimi me Postën Shqiptare.
- Marrëveshje Bashkëpunimi me Akademinë e Forcave të Armatosura.
- Marrëveshje Bashkëpunimi me Shoqatën Shqiptare të Bankave (AAB).
- Marrëveshje Bashkëpunimi me Izraelin.
- Memorandum Mirëkuptimi me Këshillin e Sigurisë Kibernetike të Emirateve të Bashkuara Arabe.
- Memorandum Mirëkuptimi me 4IG.

III. DREJTORIA E CERTIFIKIMIT, POLITIKAVE DHE ÇËSHTJEVE LIGJORE

Drejtoria e Certifikimit, e Politikave dhe e Çështjeve Ligjore, ka si objekt të veprimtarisë së saj krijimin e një mjedisi të sigurt kibernetik në rrjetet dhe sistemet e informacionit, si dhe garantimin e sigurisë së transaksioneve elektronike, duke përdorur shërbimet e besuara nëpërmjet hartimit të politikave dhe projekt akteve ligjore të nevojshme në linjë me objektivat e Autoritetit.
Drejtoria e Certifikimit, e Politikave dhe e Çështjeve Ligjore përbëhet nga drejtori i drejtorisë dhe dy struktura përkatëse:

- Sektori i certifikimeve dhe i konformitetit;
- Sektori i politikave dhe i çështjeve ligjore.

SEKTORI I CERTIFIKIMEVE DHE KONFORMITETIT

1. Trajnime dhe aktivitete pjesëmarrje në:
    - Në trajnimin e *"CompTIA Security+"* realizuar në datat 20 - 24 shkurt 2023;
    - Në aktivitetin e *"Assistance to the Albanian National Security Agency"* organizuar nga Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar në bashkëpunim TAIEX në datat 24 - 28 prill 2023;
    - Në aktivitetin e *"Qeverisjes së Krizës Kibernetike"* organizuar nga AKCESK në bashkëpunim me CRDF Global dhe organizatën C3I Cyber Security, Corporate Security and Crisis Management Initiative në datat 11 - 12 korrik 2023.
2. Është realizuar identifikimi i proceseve, hapave dhe akteve nënligjore për të përmbushur misionin e Sektorit të Certifikimeve dhe Konformitetit;
3. Është bërë një kërkim mbi modele, lidhur me përgatitjen e dokumenteve për aktet nënligjore, në kuadër të projektligjit "Për Sigurinë Kibernetike" dhe projektligjit për "Identifikimin Elektronik dhe Shërbimet e Besuara.
4. Në kuadër të projektligjit "Për Sigurinë Kibernetike" është hartuar i draft dokumenti:
    - *Pyetësor i Auditimit pranë Infrastrukturave Kritike dhe të Rëndësishme të Informacionit"* (transpozimi i ISO 27001- 2022).
    - *Udhëzim mbi përcaktimin e procedurës dhe kritereve të aplikimit për regjistrimin e organeve të vlerësimit të konformitetit pranë Autoritet Kombëtar për Sigurinë Kibernetike.*
5. Në kuadër të projektligjit "Për Identifikimin Elektronik dhe Shërbimet e besuara" është hartuar i draft dokumenti:
    - *Udhëzim mbi përcaktimin e procedurës dhe kritereve të aplikimit për regjistrimin e organeve të vlerësimit të konformitetit Autoritet Kombëtar për Sigurinë Kibernetike.*
6. Është filluar procesi i shqyrtimit të dokumentacionit për subjektin, i cili ka paraqitur kërkesën për të përfituar statusin si ofrues i kualifikuar i shërbimit të besuar.
7. Hartimi i shkresave, Memo sipas nevojave të institucionit dhe kërkesave të titullarit.

SEKTORI I POLITIKAVE DHE ÇËSHTJEVE LIGJORE

Përgjatë vitit 2023 Sektori i Politikave dhe Çështjeve Ligjore ka realizuar detyrat e mëposhtme:

1. Në kuadër të procesit të integrimit të vendit në Bashkimin Evropian ka vazhduar puna për përditësimin e bazës aktuale ligjore, ku përfshihen Ligji Nr. 9880/2008, "Për nënshkrimin elektronik", Ligjin Nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara", në harmonizim të plotë me Rregulloren Evropiane eIDAS Nr. 910/2014, "Për identifikimin elektronik dhe shërbimet e besuara për transaksione elektronike në tregun e brendshëm", si dhe Ligji Nr.2/2017, "Për sigurinë kibernetike" në harmonizim në një nivel të lartë me Direktivën Nr.2022/2555 të Parlamentit dhe Këshillit, datë 14 dhjetor 2022, "Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, e cila ka ndryshuar Rregulloren (BE) Nr.910/2014 dhe Direktivën (BE) Nr.2018/1972, si dhe ka shfuqizuar Direktivën (BE) Nr.2016/1148. (NIS 2).

   Projektligji "Për sigurinë kibernetike" u pasi u krye procesi i konsultimit publik në Regjistrin elektronik të konsultimit publik dhe takimeve me grupet e interesit, u dërgua në Kryeministri në dhjetor të vitit 2023 për vijimin me procedurat e mëtejshme për miratimin e këtij të fundit.

   Projektligji "Për identifikimin elektronik dhe shërbimet e besuara", ka përfunduar procesi i konsultimit publik (7.12.2022-10.01.2023.). Pas përfundimit të konsultimit publik u vijua me reflektimin e komenteve të ardhura nga institucionet dhe drafti final i projektligjit u dërgua elektronikisht në Kryeministri më datë 7.04.2023 për vijimin me procedurat e mëtejshme. Projektligji do rishikohet në tërësinë e tij marrë në konsideratë natyrën teknike të elementëve përbërës dhe në kuadër të riinxhinierimit të shërbimeve.

2. Aktet ligjore të miratuara gjatë vitit 2023:

   - Rregullorja e brendshme "Për organizimin dhe funksionimin e AKCESK", miratuar me Urdhrin Nr.201 datë 20.11.2023.
   - Udhëzimi Nr.2, datë 13.11.2023, "Për disa ndryshime në udhëzimin Nr.1, datë 15.03.2023, "Mbi përfundimin e aktivitetit të Ofruesit të Kualifikuar të Shërbimit të Besuar dhe Transferimin e Shërbimit"

3. Në kuadër të integrimit në Bashkimin Evropian është dhënë kontribut në këto hapësira:
   - Raportim mbi kapitujt 10, 20, 24, 31 në kuadër të GNPIE;
   - Pjesëmarrje në takime në kuadër të GNPIE;
   - Plotësim dhe raportim mbi PPAP dhe PKIE 2023-2025, 2024-2026;
   - Raportim në kuadër të hartimit të Udhërrëfyesit të Shetit të së Drejtës për kapitujt 23, 24.
   - Plotësim dhe raportim lidhur me PSIE (Paketën e Semestrit të Integrimit Evropian)
   - Përgatitja e materialit për takimet e nën komitetit të inovacioni, shoqëria e informacionit, politikat sociale (takimet 14 dhe 15).
   - Pjesëmarrja në takimet bilaterale, në Bruksel, për Kapitullin 10;

4. Draftimi, rishikimi, përmirësimi i marrëveshjeve në nivel kombëtar dhe në nivel kombëtar në fushën e sigurisë kibernetike.

Përgjatë vitit 2023 janë nënshkruar 10 marrëveshje bashkëpunimi (kombëtare) dhe 3 MoU (Memorandum Mirëkuptimi)

5. Ndjekja e proceseve gjyqësore ku Autoriteti është pale në gjyqe.
   Gjatë vitit 2023 janë zhvilluar 4 gjyqe prej te cilave 3 kanë përfunduar dhe janë fituar nga AKCESK, 1 në proces, gjykata shpalli mos kompetencën dhe ia kaloi gjykatës kompetente.

6. Hartim raportesh ligjore korrespondenca shkresore të ndryshme me institucionet sipas nevojës si dhe raportime sa herë që kërkohet në përputhje me veprimtarinë e institucionit.

7. Në kuadër të detyrimeve të përcaktuara në legjislacionin për deklarimin e pasurisë dhe parandalimin e konfliktit të interesit, është raportuar në mënyrë periodike dhe vjetore pranë ILDKPKI.

8. Marrja pjesë në:
   - ✓ Konferencën rajonale Projekti Cyber Balkans mbi Ligjin Ndërkombëtar të Sigurisë Kibernetike të BE-së 20-22 nëntor, Podgoricë ("Regional conference Cyber Balkans project on EU International Cybersecurity law").
   - ✓ "Workshop mbi Krizën Kibernetike", 11-12 Korrik, Tiranë (Governing Cyber Crisis Workshop).

   Seminar "Mbi legjislacionin kombëtar mbi sigurinë kibernetike" 6-7 Qershor, Tiranë (Seminar on National Cybersecurity Legislation)
   - ✓ Forumi i 3 i Shërbimeve të Besuara të KE-së (EC-3rd Countries Trust Services Forum).
   - ✓ Workshop iPROCEEDS-2 mbajtur në datat 26-27 Shtator 2023 në Tiranë.

IV. DREJTORIA E QEVERISJES SË SIGURISË KIBERNETIKE, KONTROLLIT DHE ZHVILLIMIT STRATEGJIK

Drejtoria e Qeverisjes së Sigurisë Kibernetike, Kontrollit dhe Zhvillimit Strategjik ka si objekt të veprimtarisë të saj sigurimin e mirëqeverisjes së sigurisë kibernetike nëpërmjet hartimit të planeve strategjike dhe monitorimit të tyre, identifikimit të infrastrukturave të informacionit dhe kategorizimit të tyre, hartimit të masave te sigurisë kibernetike për infrastrukturat e informacionit, kontrollit dhe monitorimit te tyre, ndërgjegjësimit dhe rritje e kapaciteteve, si dhe monitorimit të veprimtarisë së ofruesve te kualifikuar të shërbimit të besuar për garantimin e transaksioneve elektronike në tregun e brendshëm, nëpërmjet përdorimit të shërbimeve të besuara.

Drejtoria e Qeverisjes së Sigurisë Kibernetike, Kontrollit dhe Zhvillimit Strategjik:

1. Sektori i qeverisjes së sigurisë kibernetike dhe kontrollit;
2. Sektori i zhvillimit strategjik, komunikimit dhe identifikimit të infrastrukturave;
3. Sektori i statistikës, i modeleve dhe i analizës së indikatorëve.

SEKTORI I QEVERISJES SË SIGURISË KIBERNETIKE DHE KONTROLLIT

Në përmbushje të detyrave funksionale si dhe në zbatim të Ligjit Nr. 2/2017, "Për Sigurinë Kibernetike", Vendimit të Këshillit të Ministrave Nr. 553, datë 15.07.2020, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", i ndryshuar, dhe rregullores "**Mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë** *(V. 2.0, miratuar me Urdhrin Nr. 10/2022)*", sektori i qeverisjes së sigurisë kibernetike dhe kontrollit gjatë periudhës **Janar-Dhjetor 2023**, ka kryer kontrolle të vazhdueshme të sigurisë kibernetike pranë infrastrukturave kritike dhe të rëndësishme të informacionit.

Përgjatë vitit 2023 u **katërfishua** numri i kontrolleve me vajtje në vend, në infrastrukturat kritike dhe të rëndësishme të informacionit.

Më poshtë paraqiten në mënyrë të përmbledhur kontrollet e sigurisë kibernetike të realizuara nga Sektori i qeverisjes së sigurisë kibernetike dhe kontrollit, për vitin 2023.

Operatorët	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.

RREGULLORJA MBI PËRMBAJTJEN DHE MËNYRËN E DOKUMENTIMIT TË MASAVE TË SIGURISË V.2.0 DHE MASAT TEKNIKE KRYESORE SHTESË (BASELINE)

Sektori i qeverisjes së sigurisë kibernetike dhe kontrollit, kryen kontrolle në bazë të rregullores "**Mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë** *(V. 2.0, miratuar me Urdhrin Nr. 10/2022)*" dhe masave teknike kryesore shtesë (Baseline) të cilat duhet të implementohen nga të gjithë infrastrukturat kritike dhe të rëndësishme të informacionit në vend dhe këto masa teknike shtesë 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 rreziqeve 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.

Bazuar në rregulloren "**Mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë** *(V. 2.0, miratuar me Urdhrin Nr. 10/2022)*" dhe Baseline e masave teknike shtesë të sigurisë kibernetike, kontrolleve të ushtruara, si dhe ndjekjen (*follow up*) të infrastrukturave kritike dhe të rëndësishme, sektori i qeverisjes së sigurisë kibernetike dhe kontrollit 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.

Në bashkëpunim me infrastrukturat kritike dhe të rëndësishme të informacionit, u realizua 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 ndërgjegjësimin 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.

VETË DEKLARIMET E INFRASTRUKTURAVE KRITIKE DHE TË RËNDËSISHME TË INFORMACIONIT

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.

VLERËSIMI I DOBËSIVE TE SIGURISË KIBERNETIKE (GAP ANALYSIS)

Sektori i qeverisjes së sigurisë kibernetike dhe i kontrollit, ka realizuar vlerësimin e sigurisë të masave teknike, bazuar në masave emergjente të sigurisë dhe në Programin e Ri për vlerësimin e dobësive të sigurisë kibernetike (*GAP Analysis)*.

Përgjatë vitit 2023, u krye vlerësimi i riskut të sigurisë kibernetike në **11** institucione të rëndësishme në fushën e sigurisë dhe mbrojtjes.

Sektori i Qeverisjes së Sigurisë Kibernetike dhe Kontrollit ka implementuar **CISA CSET TOOL** për vlerësimin e nivelit te implementimit të masave të sigurisë të OIRI & OIKI

Funksionalitetet e CSET TOOL

- Kontrolli efektiv i implementimit të masave të sigurisë nga OIKI dhe OIRI
- Analizimi i dobësive të sigurisë kibernetike të OIKI dhe OIRI

- Vlerësimi i nivelit të sigurisë kibernetike (Cyber Resilience), si dhe vlerësimi i riskut të OIKI dhe OIRI
- Krijimi i profileve të dedikuara për të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit, sipas sektorëve specifikë
- Gjenerimi i raporteve (në mënyrë statistikore/grafike) për nivelin e sigurisë kibernetike të infrastrukturave
- Rekomandime për përmirësimin e dobësive të evidentuara gjatë kontrolleve

SANKSIONET ADMINISTRATIVE

Sektori i qeverisjes së sigurisë kibernetike dhe kontrollit, gjatë vitit 2023 ka hartuar "*Udhëzimi për metodologjinë e përcaktimit të dënimeve administrative në procesin e kontrollit të infrastrukturave kritike dhe të rëndësishme të informacionit*", miratuar nga Drejtori i Përgjithshëm me Nr.179 Prot., datë 03.03.2023.
Pas kryerjes së procesit të kontrollit "Mbi evadimin e zbatimit të rekomandimeve dhe masave korrigjuese si dhe verifikimi i implementimit të disa masave teknike", janë sanksionuar me gjobë:

Infrastruktura	**Numri**	**Të ardhura për buxhetin e shtetit nga gjobat**
Infrastruktura Kritike të Informacionit	4	**3 600 000 LEKË**
Infrastruktura të Rëndësishme të Informacionit	2	

KONTROLLI I OFRUESVE TË KUALIFIKUAR TË SHËRBIMIT TË BESUAR

Ofruesit e Kualifikuar të Shërbimit të Besuar (**OKSHB**) kanë detyrimin ligjor të raportojnë periodikisht mbi veprimtarinë e tyre pranë AKCESK.

OKSHB AKSHI

Përgjatë periudhës **Janar-Dhjetor 2023,** OKSHB AKSHI ka lëshuar:
5293 Certifikata elektronike me nënshkrim elektronik për Administratën Publike
18504 Certifikata elektronike me nënshkrim elektronik për Subjektet Private
3834 Certifikata elektronike për sistemin e-receta
102792 Certifikata Elektronike për projektin e fiskalizimit për subjektet private production
800 Certifikatat elektronike për projektin e fiskalizimit për institucionet shtetërore production
2700 Vula e elektronike për administratën publike

TRAJNIME

Sektori i Qeverisjes së Sigurisë Kibernetike dhe Kontrollit, ka realizuar gjatë vitit 2023 trajnime të dedikuara me operatoret e infrastrukturave kritike te informacionit dhe infrastrukturave e rëndësishme të informacionit, te identifikuar për herë të parë në VKM Nr. 761, datë 12.12.2022.

Fokusi i trajnimeve ishte në çështjet e mëposhtme:

- Njohje me kuadrin ligjor te sigurisë kibernetike në Republikën e Shqipërisë
- Plani i Ri Strategjik për Sigurinë Kibernetike
- Menaxhimi i ciklit të jetës së CSIRT
- Përfitimet e ngritjes së CSIRT
- Kategorizimi i incidenteve kibernetike
- Masat organizative dhe teknike të sigurisë që duhen implementuar nga OIRI dhe OIKI
- Kontrollet e Sigurisë Kibernetike

SEKTORI I ZHVILLIMIT STRATEGJIK, KOMUNIKIMIT DHE IDENTIFIKIMIT TË INFRASTRUKTURAVE

Sektori i zhvillimit strategjik, komunikimit dhe identifikimit të infrastrukturave ka përgjegjësi të rëndësishme për sigurinë kibernetike, duke identifikuar dhe klasifikuar infrastrukturat e reja kritike dhe të rëndësishme të informacionit dhe harton draftin e Strategjisë Kombëtare për Sigurinë Kibernetike. Gjithashtu koordinon punën me institucione të tjera për monitorimin dhe implementimin e Planit të Veprimit të Strategjisë Kombëtare për sigurinë kibernetike. Duke ndërmarrë veprime për rritjen e kapaciteteve dhe sigurisë kibernetike në vend. Planifikon dhe organizon trajnime specifike si dhe takime me aktore kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike. Ndër objektivat kryesore janë arritur si me poshtë:

ZHVILLIMI STRATEGJIK

- **Kontributi për Strategjinë Kombëtare të Sigurisë**: Sektori është angazhuar në procesin e hartimit të Strategjisë Kombëtare të Sigurisë, të udhëhequr nga Ministria për Evropën dhe Punët e Jashtme, duke dhënë kontribut lidhur me çështjet e sigurisë kibernetike, krimit kibernetik dhe diplomacisë kibernetike sipas shtyllave përkatëse të draftit të strategjisë. Kontributi i AKCESK është përfshirë në dokumentin e Strategjisë Kombëtare të Sigurisë.
- **Raporti i Monitorimit të Strategjisë Kombëtare për Sigurinë Kibernetike**: Sektori ka hartuar Raportin e Monitorimit të Strategjisë Kombëtare për Sigurinë Kibernetike për vitin 2022, pas realizimit të analizës së bërë sa i përket zbatimit të Planit të Veprimit 2020-2025. Në kuadër të këtij procesi, u monitorua realizimi i aktiviteteve të planifikuara për secilin nga institucionet përgjegjëse për implementimin e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, për katër qëllimet e politikës duke dhënë një përshkrim të aktiviteteve të realizuara si dhe duke nxjerrë përfundimet dhe rekomandimet përkatëse. Ky proces është realizuar në bashkëpunim me aktorët e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, të cilët në përgjigje të shkresave të dërguara nga AKCESK, kanë mundësuar informacion mbi realizimin e aktiviteteve të marra përsipër nga ana e tyre në përputhje me qëllimet dhe objektivat e strategjisë.
- **Përgatitja e Planit të Veprimit për SKSK 2024-2025, si dhe koordinimi i punës dhe takimet me institucionet përkatëse lidhur me këtë proces**.
  Sektori ka punuar intensivisht për hartimin e Planit të Veprimit 2024-2025 duke identifikuar prioritetet dhe nevojat sa i përket sigurisë kibernetike në nivel kombëtar, bazuar edhe në nivelin aktual të realizimit

të aktiviteteve të Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, me qëllim planifikimin e aktiviteteve dhe angazhimeve të reja që duhet të realizohen në përputhje me qëllimet dhe objektivat e Strategjisë Kombëtare për Sigurinë Kibernetike. Në këtë kuadër, ekipi i sektorit është koordinuar edhe me institucionet përgjegjëse për zbatimin e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 dhe institucionet e reja të përfshira, për të përcaktuar në bashkëpunim aktivitetet për secilin prej tyre sipas objektivave specifike dhe nevojave. Aktualisht Plani i ri i Veprimit për SKSK 2024-2025 është në proces për miratim.

INTEGRIMI EVROPIAN

Sektori ka realizuar raportime në kuadër të procesit të integrimit evropian për takimin e planifikuar të ***Nënkomitetit 14****, "****Inovacioni, Shoqëria e Informacionit, dhe Politikat Sociale",*** si dhe ***kapitullin 10 "Shoqëria e Informacionit dhe Media****" dhe* ***kapitullin 20 "Ndërmarrjet dhe Politikat Industriale"***, ku gjatë procesit të shqyrtimit analitik të acquis përkatëse janë kryer raportime periodike, si dhe është raportuar në takimin bilateral për Nënkomitetin në Shkurt 2023 online, kurse për kapitullin 10 dhe 20, takimet bilaterale u zhvilluan në zyrat e Komisionit Evropian në Bruksel, ku u raportuar mbi kornizën institucionale, politikat aktuale, kuadrin ligjor dhe planet për të ardhmen në terma të forcimit të sigurisë kibernetike në nivel kombëtar.

METODOLOGJIA PËR IDENTIFIKIMIN DHE KLASIFIKIMIN E INFRASTRUKTURAVE TË INFORMACIONIT

Sektori ka hartuar draft-Metodologjinë e re për Identifikimin dhe Klasifikimin e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit në përputhje me udhëzimet e Bashkimit Evropian dhe Direktivën (BE) 2022/2555. Kjo metodologji synon të përcaktojë hapat dhe kriteret e identifikimit dhe klasifikimit të infrastrukturave të informacionit duke u nisur nga shërbimi kritik. Në funksion të punës për hartimin e dokumenteve plotësuese të metodologjisë të tilla si bllok-skemat e klasifikimit të infrastrukturave, është hartuar pyetësori i ri në përputhje me kriteret dhe treguesit e përcaktuar në draftin e metodologjisë. Në kuadër të punës për përcaktimin e pragjeve për çdo sektor kritik sipas kritereve dhe treguesve të vendosur për klasifikimin e infrastrukturave, janë dërguar shkresa drejt disa prej operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit ekzistues për të marrë informacionet e nevojshme në përputhje me draft-Metodologjinë e re të Identifikimit dhe Klasifikimit të Infrastrukturave të Informacionit. Në vijim edhe të disa proceseve konsultimi të realizuara në vitin 2024, do të bëhet analiza e të dhënave të mbledhura për hartimin e draftit final të metodologjisë duke përfshirë kriteret dhe pragjet e përcaktuara për shërbimet kritike.

SEKTORI I STATISTIKËS, I MODELEVE DHE I ANALIZËS SË INDIKATORËVE.

Sektori i Statistikës, Modeleve dhe Analizës së Indikatorëve kryen këto detyra:

a. Analizon indikatorët e sigurisë kibernetike me qëllim identifikimin e trendeve, modeleve dhe kërcënimeve potenciale kibernetike;
b. Përpunon e administron të dhënat statistikore sipas funksioneve të Autoritetit;

c. Zhvillon dhe implementon modele efektive për shpërndarjen e informacioneve për praktikat më të mira të sigurisë kibernetike, në harmonizim me praktikat ndërkombëtare të fushës;
d. Administron dhe menaxhon të dhënat e përcjella nga sistemet e monitorimit dhe analizës, në lidhje me sistemet e administruara nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit;
e. Ngre modele të kërcënimit bazuar në statistikat e infrastrukturave kritike dhe bën parashikimin e rrezikut të sigurisë mbi këto infrastruktura;
f. Harton dhe publikon të gjitha ngjarjet dhe zhvillimet më të fundit në fushën e sigurisë, si dhe përgatit e publikon buletinet javore e mujore.

Përgjatë vitit 2023 sektori i statistikës, modeleve të analizës dhe indikatorëve ka realizuar detyrat e mëposhtme:

Në zbatim të legjislacionit në fuqi të fushës së sigurisë kibernetike, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) ka përgatitur në total:

- 12 raporte mujore,
- 4 raporte 3-mujore, dhe
- 1 raport vjetor, përgjatë vitit 2023 si nevojë për të pasqyruar vulnerabilitetet e infrastrukturave të rëndësishme dhe kritike të informacionit në ekosistemin kibernetik në nivel kombëtar, duke përcaktuar kundërmasat e sigurisë kibernetike rast pas rasti.

Janë përdorur burime dhe platforma të autorizuara për të monitoruar vulnerabilitet dhe për të vlerësuar nivelin e sigurisë së OIKI dhe OIRI, por edhe të institucioneve të tjera. Infrastrukturat e monitoruara i përkasin sektorëve të transportit, bankar, infrastrukturave digjitale, financiare, energjitike dhe sektorit publik.

Këto raporte pasqyrojnë nga pikëpamja statistikore, të dhënat e monitorimit të kryer, duke analizuar dhe kategorizuar rezultatet e gjetjeve sipas sektorëve, vulnerabiliteteve, dhe vektorëve të rrezikut, përgjatë vitit 2023. Raportet gjithashtu identifikojnë problematikat sipas sektorëve në përgjithësi, adresimin e nevojave për rritje kapacitetesh, për investim dhe teknologji.

Raportet janë bazuar vetëm në skanimin dhe analizën e kampionëve, të cilët i janë vendosur në dispozicion Autoritetit. Këto raporte nuk garantojnë të gjitha rastet e mundshme vulnerabël të OIKI/OIRI, për shkak të hapësirës së kufizuar për analizë, që ka pasur në dispozicion AKCESK.

VLERËSIMI I SIGURISË KIBERNETIKE NË NIVEL SEKTORIAL

Sektori i Statistikës, Modeleve dhe Analizës së Indikatorëve, 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.

AKTIVITETE

Materiale promovuese

Përgjatë vitit 2023 në zbatim të planit të komunikimit me publikun u krye realizimi dhe publikimi në rrjetet sociale të *Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike* i materiale promovuese për ndërgjegjësimin e komunitetit për rritjen e nivelit të sigurisë kibernetike.

Gjithashtu, periodikisht janë hartuar dhe publikuar buletine, lajme dhe artikuj, bazuar në analizën e situatës aktuale të ICT dhe sigurisë kibernetike, në kanalet zyrtare të komunikimit në media sociale të Autoritetit.

BULETINE MUJORE/ JAVORE

Përgjatë vitit 2023 janë përgatitur:

- 12 buletine mujore;
- 50 buletine javore.

<table>
<tr>
<td>Janar 2023
 
</td>
<td>Shkurt 2023
 
</td>
<td>Mars 2023
 
</td>
</tr>
<tr>
<td>Prill 2023
 
</td>
<td>Prill 2023
 
</td>
<td>Maj 2023
 
</td>
</tr>
</table>

Maj 2023

Qershor 2023

Qershor 2023

Korrik 2023

Korrik 2023

Gusht 2023

Gusht 2023

Shtator 2023

Shtator 2023

V. DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Misioni i Drejtorisë së Analizës së Sigurisë Kibernetike është analizimi i rrjeteve dhe sistemeve të informacionit dhe ekzaminimit digjital të kërcënimeve te ndryshme kibernetike, për të siguruar mbrojtjen ndaj sulmeve kibernetike në Infrastrukturat Kritike dhe të Rëndësishme të informacionit.

Pjesë e misionit të drejtorisë është edhe koordinimi dhe bashkëpunimi me Infrastrukturat Kritike dhe të Rëndësishme të informacionit dhe sektorë të tjerë të angazhuar në menaxhimin e incidenteve kibernetike, për të rritur qëndrueshmërinë kibernetike dhe marrjen e masave korrigjuese shtesë për një reagim sa më të shpejtë dhe efikas ndaj incidenteve apo sulmeve kibernetike.

Drejtoria e Analizës së Sigurisë Kibernetike:

1. Sektori i analizës së programeve keqdashëse dhe ekzaminimit digjital

2. Sektori i analizës së burimeve të hapura
3. Sektori i mbrojtjes kibernetike

SEKTORI I MBROJTJES KIBERNETIKE

Sektori i mbrojtjes kibernetike me qëllim rritjen e sigurisë kibernetike, gjatë vitit 2023, ka përmbushur me sukses objektivat si mëposhtëm:

- Analizimi i Indikatorëve të Kompromentimit (IOC), të cilat janë raportime nga Infrastrukturat Kritike dhe të Rëndësishme, ekipi i monitorimit apo nga raporte të fushatave të ndryshme që merren përmes platformave *Threat Intel*. Këto analizime kanë ndihmuar në identifikimin e trendeve, modeleve dhe kërcënimeve potenciale kibernetike
- Shpërndarja e informacionit me Infrastrukturat Kritike dhe të Rëndësishme rreth Indikatorëve të Kompromentimit me qëllim rritjen e sigurisë dhe shmangien e incidenteve të mundshme.
- Përmirësimi i planit për reagimin ndaj incidenteve, duke u hartuar "Playbooks" për 11 kategoritë e incidenteve sipas ENISA.
- Ngritja e ambienteve të simulimit si
    - *Sandbox* për të analizuar skedarët keqdashës dhe për të kuptuar më tepër rreth sjelljes së këtyre skedarëve.
    - Mail Server, për simulimin e ***mail spoofing*** me qëllim raportimin e rasteve kur këto dobësi ekzistojnë.
- Bashkëpunim me ekipin e Puple Team për krijimin e skenarëve të sulmeve të mundshme për të trajnuar ekipin e monitorimit (SOC) apo ekipet e sigurisë të Infrastrukturave Kritike dhe të Rëndësishme me qëllim rritjen e nivelit të njohurive për sigurinë kibernetike. Trajnimet janë zhvilluar në formën e ushtrimeve si TTX dhe CyberDrill.
- Bashkëpunim me ekipin "Red Team", për të realizuar vlerësimin e sigurisë mbi infrastrukturat kritike dhe të rëndësishme të cilat kanë qenë plan i ekipit "Red Team" për vitin 2023.
- Hartimi dhe shpërndarja e raporteve me rekomandime për fushatat e sulmeve të evidentuara përmes kërkimeve, përmes platformave *Threat Intel* apo për dobësitë e njohura (KEV) sipas CISA.
- Mbështetje metodologjike në rastet e incidenteve me impakt të lartë duke asistuar në rikthimin e shërbimeve në kohë relativisht të shkurtër.
- Analizimi i thelluar i log-eve të raportuara nga ekipi i monitorimit dhe logeve të vendosura në dispozicion nga infrastrukturat e prekura nga incidentet kibernetike. Duke kuptuar më tej teknikat që aktorët keqdashës kanë ndjekur.
- Bashkëpunimi me ekipin e monitorimit SOC për marrjen e çdo informacioni mbi anomalitë e evidentuara gjatë monitorimit të logeve, me qëllim garantimin e shërbimeve të sigurta në teknologjinë e informacionit dhe komunikimit.
- Bazuar në të dhënat e sistemeve të monitorimit është kryer analizimi i rreziqeve kibernetike që prekin asetet e infrastrukturave kritike dhe të rëndësishme të informacionit me qëllim identifikimin dhe trajtimin e tyre për të reduktuar riskun dhe arritjen e një niveli të maturuar të sigurisë kibernetike.

SEKTORI I ANALIZËS SË BURIMEVE TË HAPURA

Në zbatim të detyrave funksionale, sektori i analizës së burimeve të hapura monitoron aktivitetet në Dark Web, analizon rreziqet nga Dark Web dhe burimet e hapura, si dhe identifikon rreziqet potenciale të aktorëve keqdashës në infrastrukturat kritike dhe të rëndësishme të informacionit.
Për të përmbushur detyrat funksionale, sektori i analizës së burimeve të hapura përdor mjete dhe burime OSINT për të kryer mbledhjen e informacionit mbi taktikat, teknikat dhe procedurat e përdorura nga aktorët keqdashës.
Me qëllim parandalimin e incidenteve potenciale në infrastrukturat kritike dhe të rëndësishme të informacionit, janë hartuar dhe shpërndarë raporte mbi:

Vulnerabilitete dhe Përditësime të Sigurisë (38 Raporte):

- **Vulnerabilitete Kritike (14 Raporte)**: Përfshirë dobësitë në Microsoft Message Queuing Service, Dell Power Manager, Cloudflare WARP Client etj.
- **Përditësime të Sigurisë (24 Raporte)**: Përditësime për Google Chrome, Android OS, produktet Cisco, McAfee Safe Connect, dhe të tjerë.

Fushatat e Malware dhe Ransomware (13 Raporte):

- **Fushatat e Ransomware (5 Raporte)**: Yashma, Monti, Farnetwork Ransomware-as-a-Service, dhe të tjera.
- **Variantet e Malware dhe Teknikat e Sulmit (8 Raporte)**: NodeStealer 2.0, Malware MetaStealer, Xloader, dhe më shumë.

Sulmet dhe Dobësitë Zero-Day (12 Raporte):

- **Sulmet Zero-Day dhe Teknikat e Sulmit (6 Raporte)**: Inception Attack në AMD Zen CPU, Cisco VPN, Mozilla etj.
- **Dobësitë Zero-Day dhe Kritike (6 Raporte)**: Dobësi në software të Cisco-NX-OS, SolarWinds ARM, dhe të tjerë.

Bashkëpunimi me Sektorët e Tjerë

- Raport mbi Teknikat, Taktikat dhe Procedurat për grupet Iraniane
- Raport mbi Teknikat, Taktikat dhe Procedurat për grupet Ruse
- Raporte për grupe të tjera që kanë vepruar në Rajonin e Ballkanit Perëndimor

Zbulime të rëndësishme përfshijnë gjithashtu të dhëna sensitive, të cilat janë koordinuar rast pas rasti me autoritetet përgjegjëse të fushës, si Policia e Shtetit dhe Komisioneri për të drejtën e informimit dhe mbrojtjen e të dhënave personale.

SEKTORI I ANALIZËS SË PROGRAMEVE KEQDASHËSE DHE EKZAMINIMIT DIGJITAL

Në zbatim të detyrave funksionale, sektori i Analizës së programeve keqdashëse dhe ekzaminimit digjital kryen analizën e programeve keqdashëse dhe ekzaminimin digjital të incidenteve kibernetike, me qëllim mitigimin e efekteve të dëmshme në rrjetet dhe sistemet e afektuara, marrjen e masave për rikuperim e

dëmeve të shkaktuara si dhe parandalimin e incidenteve te tjera të ngjashme në të gjitha rrjetet dhe infrastrukturat e informacionit.

Gjatë periudhës Janar-Dhjetor 2023, Sektori i Analizës së programeve keqdashëse dhe ekzaminimit digjital ka përmbushur me sukses disa nga objektivat kyçe në përmbushje të detyrave funksionale të tij:

- Ka ekzaminuar, identifikuar dhe kuptuar natyrën e kërcënimeve kibernetike të ndryshme si viruset, worms, bots, rootkits, dhe Trojan. Gjithashtu ka identifikuar kërcënimet kritike që rrjedhin nga sulmet si pasojë e Zero-Day dhe Ransomware Attack.
- Ka asistuar në mbështetje teknike dhe metodike mbi sulmet e ndodhura si dhe ka realizuar raporte teknike post-analizë për të gjitha incidentet e ndodhura, duke nxjerrë përfundime, rekomandime dhe masat specifike për të parandaluar incidente të ngjashme.
- Të gjitha raportet teknike post analize për incidentet e ndodhura, masat rekomanduese dhe parandaluese i janë përcjelle infrastrukturave kritike dhe të rëndësishme te informacionit në kohë reale nëpërmjet kanaleve të sigurta të komunikimit.
- Ka përgjigjur me asistencë të menjëhershme teknike ndaj incidenteve të sigurisë që janë raportuar në Autoritet, duke ofruar ndihmë deri në zgjidhjen e tyre dhe analiza të detajuara post-incidenti.
- Ka kryer kërkime të vazhdueshme për zhvillimet në fushën e sigurisë kibernetike dhe ka rekomanduar përditësime të sigurisë në rastet kur janë konstatuar vulnerabilitete. Numërohen mbi 200 raporte të përcjella drejt infrastrukturave kritike dhe te rëndësishme te informacionit vetëm për 6 mujorin e pare te vitit, numër ky ne rritje për 6 mujorin e dyte. Një pjesë e mire e raporteve janë hartuar me ndihmën e burimeve dhe partnereve ndërkombëtare.
- Ka bashkëpunuar ngushtë me ekipet e tjera të institucionit për të krijuar një raport të qartë të problemeve të sigurisë në infrastrukturat që janë testuar. Vlen të theksohet qe sektori ka kontribuar ne rritjen e kapaciteteve te SOC kombetar duke kryer vazhdimisht Table Top Exersice dhe Cyber Drills per SOC.
- Ka marrë pjesë në ushtrime gatishmërie si purple team, table top exercises, cyber drills te cilat kanë stërvitur ekipet e sigurisë te infrastrukturave kritike dhe të rëndësishme të informacionit, institucioneve të pavarura, universiteteve etj. Konkretisht disa prej trajnimeve të kryera janë :
  - TTX dhe CyberDrill per Sektorin Energjitik dhe Transportin
  - TTX dhe CyberDril per sektorin Financiar
  - Trajnim online me te gjitha infrastrukturat ne Shqiperi
  - Trajnim mbi analizen e proceseve ne sistemet operative Windows dhe Linux gjate periudhes se sulmeve te muajit dhjetor 2023
- Ka ekzaminuar incidentet e ndodhura në Infrastrukturat Kritike dhe të Rëndësishme duke përdorur mjetet për Malware Analysis dhe Digital Forensics. Konkretisht ka arritur të menaxhoje 49 incidente kibernetike te raportuara prej të cilave 12 janë klasifikuar me impakt të larte.
- Ka dhënë kontribut të rëndësishëm në përgatitjen e akteve ligjore dhe nënligjore që lidhen me fushën e veprimtarisë së Autoritetit. Përkatësisht ka dhëne kontribut ne hartimin e Procedurës se incidenteve kibernetike, krijimin e Playbook-eve, hartimin e Procedurës se Krizes Kibernetike etj.

- Ka marrë masa të shpejta dhe efikase për reagimin ndaj vulnerabiliteteve të konstatuara për të parandaluar dhe menaxhuar incidentet e mundshme kibernetike.
- Ka prodhuar raporte periodike ose ad-hoc të cilësisë së lartë për incidentet, kërcënimet e sigurisë dhe vulnerabilitetet e zbuluara disa prej te cilave përmenden si me poshtë:
  - Raport dhe analize për një fushate te re nga APT34
  - Raport dhe analize për një fushate sulmesh drejt Amazon S3
  - Raport mbi një fushate sulmesh nga CharmingKItten
  - Raport dhe analize për një fushate sulmesh nga Winter Vivern
  - Raport mbi një fushate sulmesh nga APT Kineze
  - Raport dhe analize për një fushate phishing nga MuddyWater
  - Raport mbi një fushate nga APT29 qe shenjestron ambasadat.
  - Raport mbi një fushate te re sulmesh Agent Racoon
  - Analize dhe raport për Ransomware Lockbit 3.0
  - Raport mbi TTP e Homeland Justice
  - Analize dhe raport mbi malware Kurs Trajnimi.Zip
  - Analize mbi grupet ruse
  - Raport dhe analize mbi sulmin ddos të APT Ruse

- Ka përfaqësuar Autoritetin në konferenca ndërkombëtare dhe ka marrë pjesë në grupe pune dhe takime brenda vendit dhe brenda institucionit. Ka drejtuar CSIRT kombëtar ne stërvitjen kibernetike “Cyber Coalition 2023” ne NATO.

- Ka realizuar me sukses implementimin e disa prej platformave më të rëndësishme, të cilat kanë kontribuar ndjeshëm në përmirësimin dhe efikasitetin e proceseve të punës.

- Ka mundësuar ngritjen e një platforme për ruajtjen e të dhënave duke automatizuar procesin e kërkimit manual të hasheve, IP-ve apo url-ve. Kjo platforme ka ndihmuar në krijimin e raporteve ditore ne format excel të IOC të ruajtura nga SOC Kombëtar, ruajtjen e tyre duke krijuar një historik, si dhe ndihmën e analizave me te thelluara te tentativave për sulme në OIRI/OIKI.
- Ka koordinuar efektivisht komunikimet me institucione të tjera ligj zbatuese për marrjen e masave emergjente për parandalimin e incidenteve kibernetike. Gjatë këtij procesi, ka raportuar një numër të lartë të IP-ve malinje, domaineve jo legjitimë dhe faqeve të internetit të dëmshme.

VI. DREJTORIA E QENDRËS OPERACIONALE-CSIRT

Drejtoria e Qendrës Operacionale ka si objekt të veprimtarisë së saj sigurimin e një niveli të lartë të sigurisë kibernetike të rrjeteve dhe sistemeve, nëpërmjet monitorimit të tyre dhe ndërveprimit, simulimeve të vazhdueshme, me qëllim rritjen e qëndrueshmërisë kibernetike dhe marrjen e masave korrigjuese shtesë, për një reagim sa më të shpejtë dhe efikas ndaj incidenteve apo sulmeve që mund të afektojnë infrastrukturat kritike dhe të rëndësishme të Informacionit.
Drejtoria e Qendrës Operacionale (CSIRT) përbëhet nga Drejtori i Drejtorisë dhe dy sektorët:

- Sektori i Monitorimit dhe Reagimit të Incidenteve Kibernetike (SOC 1 & SOC);

- Sektori i Simulimeve të Incidenteve Kibernetike.

Në përmbushje të veprimtarisë së saj Drejtoria e Qendrës Operacionale bashkërendon dhe koordinon monitorimin, reagimin, menaxhimin dhe trajtimin e incidenteve kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit, me qëllim parandalimin e incidenteve kibernetike në to dhe mbrojtjen e tyre, siguron ndihmë dhe mbështetje metodike për operatorët përgjegjës në fushën e sigurisë kibernetike, si dhe kryen simulime të ndryshme incidentesh dhe sulmesh me qëllim rritjen e kapaciteteve teknike dhe operacionale në nivel kombëtar.

SEKTORI I MONITORIMIT DHE REAGIMIT TË INCIDENTEVE KIBERNETIKE (SOC1 & SOC2)

Në zbatim të detyrave funksionale, sektori i monitorimit dhe reagimit të incidenteve kibernetike (SOC1 & SOC2) kryen monitorim të rrjeteve dhe sistemeve të informacionit 24/7, menaxhon dhe trajton në kohë reale incidentet e mundshme kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit, duke parandaluar afektimin e shërbimeve dhe informacionit që ato administrojnë.

Sektori i monitorimit dhe reagimit të incidenteve kibernetike (SOC1 & SOC2) kryen bashkërendimin dhe koordinimin e punës së monitorimit, reagimit, menaxhimit dhe trajtimit të incidenteve kibernetike të ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit, pas kategorizimit të incidenteve të evidentuara gjatë monitorimit.

Procesi i monitorimit të SOC Kombëtar kryhet nëpërmjet platformave me agjentë dhe pa agjentë. Operatorët e monitoruar i përkasin sektorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, në zbatim të legjislacionit në fuqi, specifikisht Vendimit të Këshillit të Ministrave Nr. 553, datë 15.7.2020, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", (i ndryshuar me VKM Nr. 761, datë 12.12.2022). Në këtë kontekst, SOC Kombëtar monitoron një total prej rreth 133 operatorësh të infrastrukturave të informacionit në nivel kombëtar.

Për përmbushjen e detyrave funksionale, SOC Kombëtar monitoron IP-të publike dhe të gjitha ndërfaqet e sistemeve që kanë akses në publik duke i analizuar ato në sisteme të dedikuara që analizojnë informacione për:

a) Veprimtari keqdashëse nga këto IP/Servera (Sisteme) drejt serverëve të tjerë në internet.
b) Aktivitet nga interneti drejt IP/Serverave (Sistemeve) të infrastrukturave.

Në kohë reale SOC Kombëtar komunikon çdo anomali të evidentuar në infrastrukturat e informacionit me pikat e kontaktit të këtyre të fundit, duke siguruar ndihmë dhe mbështetje metodike për operatorët përgjegjës në fushën e sigurisë kibernetike për raste vunerabilitetesh apo anomali të konstatuara gjatë procesit të monitorimit të cilat nuk kanë nevojë për analizë të thelluar. Për të gjitha raportimet apo detektimet e tjera, SOC Kombëtar e eskalon rastin në ekipet e tjera për analizë më të thelluar.

SEKTORI I SIMULIMEVE TË INCIDENTEVE KIBERNETIKE

Në zbatim të detyrave funksionale, sektori i simulimeve të incidenteve kibernetike kryen simulime të ndryshme incidentesh dhe sulmesh me qëllim rritjen e qëndrueshmërisë kibernetike në infrastrukturat e informacionit dhe kapaciteteve teknike e operacionale të tyre.

Simulimi i sulmeve kibernetike realizohet në bazë të kalendarit të Kontrollit të Masave të Sigurisë të AKCESK, si dhe me kërkesë zyrtare nga infrastruktura. Përpara kryerjes së simulimit të sulmit kibernetik, infrastrukturës i dërgohen "Rregullat e Angazhimit dhe Qëllimi i punës", të cilat përmbajnë rregullat dhe mënyrën që do skanohet.

Infrastruktura mund të zgjedhë nëse dëshiron vetëm, Skanim Vulnerabilitetesh ose Simulim Sulmi dhe E-mail Phishing.

Gjithashtu, përpara nisjes së procesit të kontrollit pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, sektori kryen paraprakisht një vlerësim të vulnerabiliteteve të mundshme për adresat IP të vendosura në dispozicion nga vetë infrastrukturat e informacionit, duke përdorur burime të ndryshme të skanimit, të cilat ndihmojnë në identifikimin dhe trajtimin e problematikave.

Për vitin 2023 janë 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)**

Për vulnerabilitetet e identifikuara përcaktohet niveli i riskut, përshkrimi i vulnerabiliteteve dhe mënyra se si mund të kryhet mitigimi i tyre. 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 dhe gjithashtu të merren në konsideratë rekomandimet për të gjitha gjetjet shtesë.

VII. DREJTORIA E FINANCËS DHE SHËRBIMEVE MBËSHTETËSE

Drejtoria e financës dhe shërbimeve mbështetëse ka në strukturën e vet dy sektor:

- Sektori i financës
- Sektori i Burimeve Njerëzore dhe Shërbimeve Mbështetëse

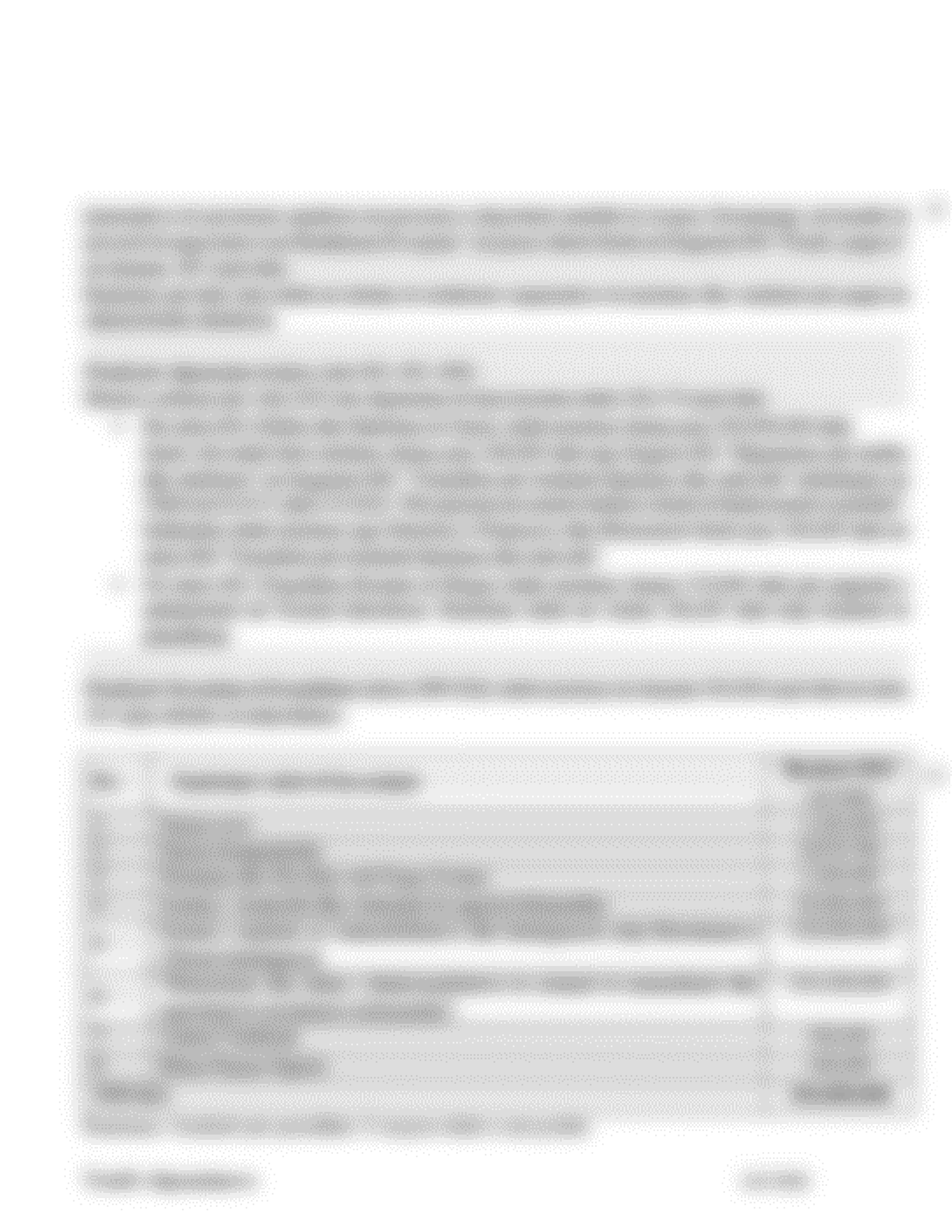
Qëllimi i drejtorisë është zbatimi i rregullave dhe ligjeve të menaxhimit të burimeve njerëzore, menaxhimin financiar dhe kontrollin në procesin e përdorimit të fondeve buxhetore , ndjekjen dhe hartimin e kërkesave buxhetore, mbajtjen e kontabilitetit të aktivitetit dhe hartimin e llogarive vjetore .
Objektivi i saj është garantimi i përdorimit të fondeve publike, nëpërmjet kryerjes së kontrollit paraprak të përputhshmërisë së operacioneve ekonomike me planin dhe legjislacionin në fuqi.

SEKTORI I FINANCËS

Në zbatim të Ligjit Nr.84/2022, "Për buxhetin e vitit 2023", Udhëzimit të Ministrit të Financave Nr.9, datë 20.02.2018, "Për procedurat standarde të zbatimit të buxhetit" i ndryshuar, Udhëzimit të Ministrisë së Financave Nr.7 datë 28.2.2018, "Për procedurat standarde të përgatitjes së PBA" si dhe të Udhëzimit të Ministrit të Financave Nr.22, datë 07.07.2023, "Për përgatitjen e Programit Buxhetor Afatmesëm 2024-2026", Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike administron dhe menaxhon fondet e vëna në dispozicion nga Buxheti i Shtetit për vitin 2023.

Për Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike buxheti i alokuar për vitin 2023 është **533,369 mijë lekë** nga të cilat 229,369 mijë lekë Shpenzime Korrente dhe 304,000 mijë lekë Shpenzime Kapitale me financim të brendshëm si më poshtë:
Plani i shpenzimeve totale (*në lekë)* sipas zërave të buxhetit është:

Nr.	**Emërtimi i zërave të Buxhetit**	**Plani i Vitit 2023**
600	Paga	113,897,050
601	Sigurime Shoqërore	15,202,000
602	Mallra dhe Shërbime të Tjera	99,894,000
603	Subvencione	
604	Transferta Korente të Brendshme	
605	Transferta Korente të Huaja	170,000
606	Trans për Buxh. Fam. & Individ	206,000
231	Shpenzime Kapitale	304,000,000
TOTALI		**533,369,050**



Emërtimi i Shpenzimeve	Buxheti Fillestar Janar -Dhjetor 2023	Buxheti Rishikuar Janar - Dhjetor 2023	Buxheti Janar – Dhjetor 2023	Fakti Janar - Dhjetor 2023	Në %
Shpenzime Korrente	238,302,000	229,369,050	229,369,050	137,022,888	59.7%
Kapitale të brendshme	304,000,000	304,000,000	304,000,000	10,754,674	3.5%
Shpenzime Totale	**542,302,000**	**533,369,050**	**533,369,050**	**147,777,562**	

SEKTORI I BURIMEVE NJERËZORE DHE SHËRBIMEVE MBËSHTETËSE

Në vijim të sigurimit të përmbushjes së misionit të Sektorit të Burimeve Njerëzore dhe Shërbimeve Mbështetëse, për menaxhimin e burimeve njerëzore dhe shërbimet mbështetëse të AKCESK, janë realizuar:

- Miratimi i përshkrimeve të punës, sipas strukturave të miratuara me Urdhër të Kryeministrit Nr. 32, datë 16.03.2023 dhe Nr. 233 datë 20.12.2023.
- Riemërimi i punonjësve aktualë të AKCESK, në pozicionet e reja e punës, sipas strukturës së miratuar me Urdhër të Kryeministrit Nr. 32, datë 16.03.2023, (20 punonjës dhe 2 specialistë praktikantë me pozicion jashtë strukture, në kuadër të Programit Kombëtar të Praktikave të Punës) dhe strukturës së miratuar me Urdhër të Kryeministrit Nr. 233 datë 20.12.2023, (48 punonjës dhe 1 specialist praktikant me pozicion jashtë strukture, në kuadër të Programit Kombëtar të Praktikave të Punës);
- Miratimi i kontratës së re individuale të punës dhe nënshkrimi i kontratave me punonjësit ekzistues dhe punonjësit e rinj të AKCESK. (Pas rishikimit të kontratës aktuale dhe ndryshimeve përkatëse, u lidhën kontratat individuale të punës, sipas strukturave të miratuara);
- Procedura e rekrutimit të punonjësve të rinj për vendet vakantë, gjatë gjithë vitit;
- Organizimi i punës, asistimi dhe bashkëpunimi me sektorët për realizimin e vlerësimit të performancës së punonjësve;
- Kontrolli i zbatimit me korrektësi i rregullave të etikës dhe disiplinës në punë dhe evidentimi i problematikave sipas Rregullores së Brendshme në fuqi;
- Menaxhimi i burimeve njerëzore lidhur me përmbajtjen dhe procedurat administrative;
- Menaxhimi i shërbimeve të brendshme të institucionit, si dhe menaxhimi i veprimtarisë së arkiv/protokollit, administrimi i lëvizjes të korrespondencës brenda dhe jashtë institucioni dhe shërbimet e tjera mbështetëse.

Referuar Urdhrit Nr. 32 datë 16.03.2023 të Kryeministrit "Për miratimin e strukturës dhe të organikës së Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike", struktura e AKCESK ka 85 punonjës e përbëhet nga 5 drejtori:

- **Drejtoria e Certifikimit, Politikave dhe Çështjeve Ligjore (**2 sektorë**).**
- **Drejtoria e Qeverisjes së Sigurisë Kibernetike, Kontrollit dhe Zhvillimit Strategjik (**3 sektorë**).**
- **Drejtoria e Analizës së Sigurisë Kibernetike (**3 sektorë**).**
- **Drejtoria e Qendrës Operacionale – CSIRT (**2 sektorë**).**
- **Drejtoria e Financës dhe Shërbimeve Mbështetëse (**2 sektorë**).**

Referuar Urdhrit Nr. 233, datë 20.12.2023, "Për miratimin e strukturës dhe të organikës së Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike", struktura e AKCESK u riorganizua në 6 drejtori:

- **Drejtoria e Certifikimit, Politikave e Legjislacionit të Sigurisë Kibernetike (**2 sektorë**).**
- **Drejtoria e Koordinimit të Projekteve Ndërkombëtare dhe Zhvillimit Strategjik të Sigurisë Kibernetike (**2 sektorë**).**
- **Drejtoria e Monitorimit dhe Reagimit të Incidenteve, Qendrës Operacionale SOC C-SIRT (**2 sektorë**).**
- **Drejtoria e Analizës së Sigurisë Kibernetike (**2 sektorë**).**
- **Drejtoria e Analizës së Përputhshmërisë, Riskut dhe Kontrollit të Masave të Sigurisë Kibernetike (**2 sektorë**).**
- **Drejtoria e Financës dhe Shërbimeve Mbështetëse (**2 sektorë**).**

Pas plotësimit të pozicioneve të punës, nga punonjësit ekzistues, ka lindur nevoja për plotësimin e pozicioneve vakante, sipas drejtorive përkatëse, procedurë e cila ka vijuar përgjatë gjithë vitit.
Referuar për sa më sipër, me qëllim plotësimin e vendeve vakante të AKCESK, janë nxjerrë 19 urdhra të brendshëm për shpallje rekrutimi, për pozicionet vakante, gjatë vitit 2023.
Është mbajtur dhe përditësuar plani i trajnimeve të punonjësve dhe pjesëmarrjeve në veprimtari të ndryshme brenda dhe jashtë vendit, përgjatë vitit 2023:

- Trajnime jashtë vendit 47
- Trajnime brenda vendit 14
- Raportime/Konferenca/Aktivitet 20