Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike

RAPORT VJETOR 2021

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

Tabela e përmbajtjes

1. Drejtoria e Certifikimit elektronik dhe Kontrollit

1.1. Sektori i Akreditimit dhe Politikave

Sektori i Akreditimit dhe Politikave ka këto përgjegjësi të përcaktuara në rregulloren e brendshme të institucionit:

a) Shqyrton dhe vlerëson dokumentacionin përkatës dhe kërkesën e dorëzuar nga subjektet për procesin e akreditimit si ofruesi i kualifikuar i shërbimit të besuar.

b) Mban kontakte të vazhdueshme me ofruesit e kualifikuar të shërbimit të besuar të akredituar pranë AKCESK, dhe kërkon plotësim dokumentacioni për çdo ndryshim teknik ose operacional që OKSHB ndërmerr.

c) Menaxhon dokumentacionin e ofruesve të kualifikuar të shërbimit të besuar dhe dokumentacionin e organizmave të testimit dhe konfirmimit, si dhe mirëmban Listat e Besuara (Trust Lists) të ofruesve të kualifikuar të shërbimeve të besuara. Publikon këto lista për ndërveprim dhe njohje reciproke të nënshkrimeve elektronike me vendet anëtarë të BE-së.

d) Raporton mbi konformitetin e dokumentacionit ligjor dhe teknik të dorëzuar nga ofruesit e kualifikuar të shërbimit të besuar, sipas kritereve të AKCESK, normave evropiane dhe standardeve teknike të ETSI (European Telecommunications Standards Institute).

e) Vlerëson plotësimin e kritereve të Politikave të Certifikimit, të Deklaratës së Praktikave të Certifikimit, Manualit Operativ dhe Politikave të Vulës Kohore.

f) Vlerëson dokumentacionin e dorëzuar për pajisjet e sigurta të krijimit të nënshkrimit dhe certifikatat e lëshuara nga prodhuesi i tyre, në mënyrë që të plotësohet niveli evropian i sigurisë.

g) Harton raportin mbi kërkesën për akreditim/regjistrim të ofruesit të kualifikuar të shërbimit të besuar dhe sugjeron pranë Drejtorit të Drejtorisë, nëse subjektit duhet t'i jepet akreditimi ose jo.

h) Harton rregulla specifike në përputhje me ndryshimet sipas standardeve ndërkombëtare, në fushën e nënshkrimit elektronik, identifikimit elektronik dhe shërbimeve të besuara dhe sigurisë kibernetike.

i) Harton akte ligjore dhe nënligjore përsa i përket fushës së certifikimit elektronik dhe sigurisë kibernetike, sipas nevojave të evidentuara të institucionit, të harmonizuara me acquis të BE-së.

j) Bashkëpunon dhe bashkërendon punën me institucione të tjera, për implementimin e nënshkrimit elektronik, identifikimit elektronik dhe shërbimeve të besuara.

k) Siguron pjesëmarrjen e punonjësve, në konferenca dhe trajnime kombëtare dhe ndërkombëtare, për rritjen e nivelit profesional të punonjësve.

l) Monitoron zbatimin e Strategjisë Kombëtare të Sigurisë Kibernetike dhe të politikave të tjera ku AKCESK është kontribues.

Përgjatë vitit 2021 sektori i Akreditimit dhe Politikave ka realizuar detyrat e mëposhtme:

1. Në kuadër te 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. 10273/2010 "Për dokumentin elektronik", Ligjin Nr. 107/2015 "Për identifikimin elektronik dhe shërbimet e besuara", si dhe Ligjin nr.2/2017 "Për sigurinë kibernetike" 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 në harmonizim të plotë me Direktivën (BE) 2016/1148 e Parlamentit Evropian dhe e Këshillit "Mbi masat për një nivel të lartë të përbashkët të sigurisë së rrjeteve dhe sistemeve të informacionit në të gjithë Bashkim Evropian" (NIS Directive).

Gjithashtu, janë hartuar dhe dorëzuar draft ligji i ri i bazuar mbi draft direktivën e re BE (NIS 2) si dhe ligji i ri bazuar mbi draft rregulloren e re Evropiane eIDAS 2.0, shoqëruar me tabelën përkatëse të përputhshmërisë.

2. Për ofruesit e kualifikuar të shërbimit të besuar të regjistruar pranë Autoritetit është kryer një rivlerësim dokumentacionit të dorëzuar prej tyre, si dhe janë azhurnuar dokumentacionet sipas standardeve ndërkombëtare në fushën e shërbimeve te besuara.

3. 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 ILDKPKIE.

4. Gjatë vitit 2021 është hartuar "Rregullorja mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë 2.0", ku përcaktohen masat e sigurisë, të drejtat, detyrimet për Operatorët e Infrastrukturave Kritike të Informacionit (OIKI) dhe Operatorëve e Infrastrukturave të Rëndësishme të Informacionit (OIRI), si dhe përcakton përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë, konform udhëzimeve më të fundit të ENISA.

5. Kontribut lidhur me ecurinë e zbatimit të masave dhe aktivitetet e parashikuara në planin e veprimit 2021-2023 të "Strategjisë ndër sektoriale të luftës kundër terrorizmit 2021-2025".

6. Në kuadër të integrimit në Bashkimin Evropian është dhënë kontribut në këto hapësira:

    - Raportim mbi kapitujt 3 dhe 10 në kuadër të GNPIE;
    - Pjesëmarrje në takime online në kuadër të GNPIE;

- Plotësim dhe raportim mbi PPAP dhe PKIE 2022-2024;

7. Administrimi i faqes zyrtare të Autoritetit www.cesk.gov.al. Përditësohet vazhdimisht dokumentacioni i faqes, përfshirë tekstet, ligjet, aktivitetet, lajmet më të fundit mbi qarkullimin e viruseve/vulnerabiliteteve të ndryshme, si dhe fushata ndërgjegjësimi për një internet më të sigurt për fëmijët dhe të rinjtë në internet .
8. Përditësimi i Listës se Besuar (Trust Lists) të ofruesve të kualifikuar të shërbimeve të besuara sipas modelit të listës së besuar të BE, me qëllim ndërveprimin dhe njohjen reciproke të nënshkrimit/identifikimit elektronik në vendet e tjera.
9. Pjesëmarrje në trajnime për rritjen e kapaciteteve teknike dhe profesionale në fushën e shërbimeve të besuara dhe sigurisë kibernetike organizuar nga FESA, ENISA etj. Pjesëmarrje në takime të zhvilluar nga Këshilli i Kooperimit Rajonal (RCC) mbi raportimin e progresit për aktivitete/çështje te planit të Veprimit për Tregun e Përbashkët (CRM 2021-2024) qe lidhen me veprimtarinë e Autoritetit.
10. Hartim raportesh ligjore si dhe korrespondenca të ndryshme sipas nevojës së institucionit.

1.2. Sektori i Komunikimit dhe Shpërndarjes së Informacionit

Sektori i Komunikimit dhe Shpërndarjes së Informacionit ka këto përgjegjësi:

a) Menaxhon procesin e hartimit të metodologjive të punës, për analizën e rrezikut kibernetik në OIKI/OIRI dhe mbikëqyr procesin e vlerësimit të tij.
b) Merr pjesë në grupin e punës për vlerësimin e rrezikut kibernetik në OIKI/OIRI.
c) Harton dhe shpërndan lajmërime paraprake mbi sigurinë e informacionit.
d) Analizon detyrat dhe angazhimet ndaj organizmave ndërkombëtare, në përputhje me politikat e institucionit.
e) Koordinon dhe përmbush detyrimet raportuese në nivel institucional mbi progres raportet e ndryshme.
f) Organizon dhe bashkërendon aktivitetet e ndryshme brenda fushës së veprimtarisë së institucionit.
g) Mban lidhje me organizmat ndërkombëtare (NATO; OSBE; FESA; ENISA; ETSI; FIRST; TI; ECSO, etj.), për përmbushjen e angazhimeve të ndërmarra nga AKCESK, në fushën e sigurisë kibernetike dhe shërbimeve të besuara.
h) Mban lidhje me institucionet kombëtare dhe ndërkombëtare, me qëllim që të përcaktojë dhe identifikojë programet e trajnimit për rritjen e kapaciteteve të punonjësve të AKCESK dhe i propozon ato tek eprori.

Përgjatë vitit 2021 sektori ka realizuar aktivitete në kuadër të rritjes së ndërgjegjësimit të komunitetit si dhe rritjes së kapaciteteve të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, me qëllim realizimin e detyrave funksionale të Autoritetit.

Aktivitete për Rritjen e Ndërgjegjësimit

1. "Dita Ndërkombëtare e Internetit të Sigurt 2021"

Në kuadër të "Ditës Ndërkombëtare të Internetit të Sigurt", Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) organizoi aktivitetin "Politikat kombëtare të rritjes së sigurisë së fëmijëvenë Internet". Ky aktivitet u realizua në bashkëpunim me International TelecommunicationUnion (ITU), në cilësinë e partnerit strategjik,si një ndër aktorët kryesorë që ka qëllim rregullimin dhe standardizimin e hapësirës kibernetike.

2. Prezantimi i "Portalit të Sinjalizimit të AKCESK"

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në vijim të takimeve për mbrojtjen e fëmijëve në internet, si një nga objektivat e "Strategjisë Kombëtare për Sigurinë Kibernetike", organizoi në datë 27 Maj 2021, takimin konsultativ, me qëllim prezantimin e ndërveprimit të aktorëve pjesëmarrës me "Portalin e Sinjalizimit të AKCESK".

Gjatë takimit, theksi u vendos në forcimin e koordinimit ndërinstitucional për trajtimin me efektivitet të rasteve të raportuara dhe zgjidhjen e problematikave të fëmijëve dhe të rinjve në internet, në lidhje me abuzimet seksuale online dhe elementët kontaminues që propagandojnë mbi radikalizimin dhe ekstremizmin e dhunshëm online.

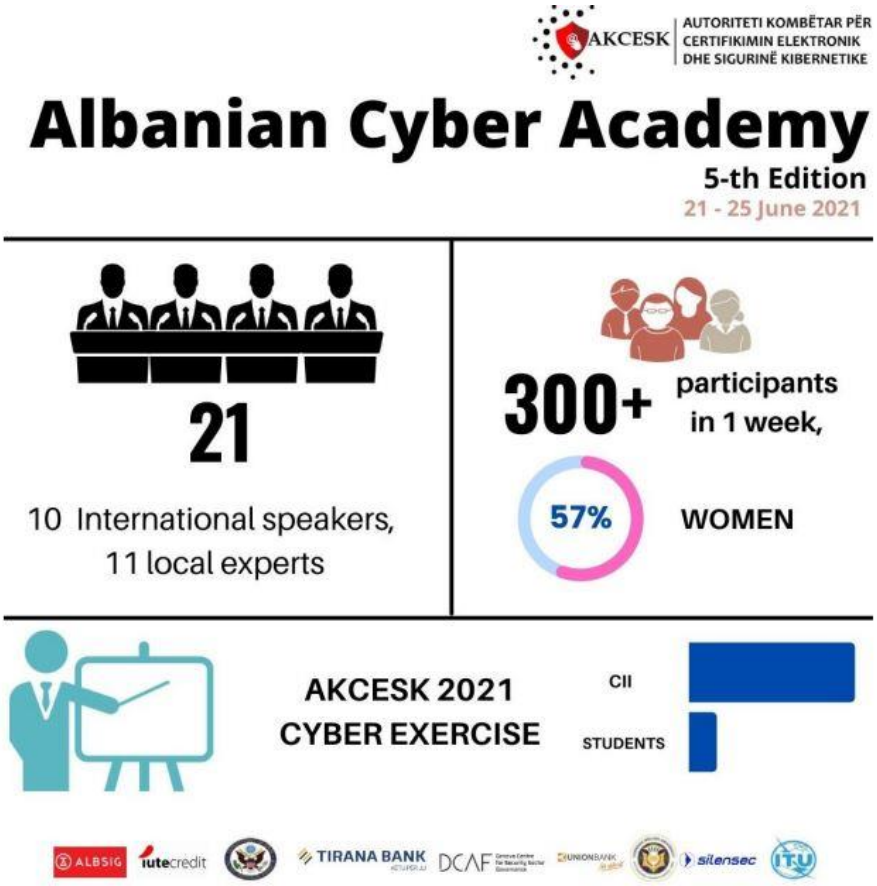
3. "Albanian Cyber Academy" Edicioni 5

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në bashkëpunim me Ambasadën e SHBA-së në Tiranë, Tirana Bank, Union Bank, Albsig Sh.a., Iute Credit, DCAF, Silensec International Telecommunication Unit, Carnegie Mellon University, organizuan në datat 21-25 Qershor 2021, edicionin e pestë të Albanian Cyber Academy (ACA5).

ACA5 synoi rritjen e kapaciteteve dhe thellimin e njohurive në fushën e sigurisë kibernetike për studentët e viteve të fundit të degëve TIK dhe operatorëve të infrastrukturave kritike të informacionit.

Edicioni i pestë i Albanian Cyber Academy kishte të ftuar 10 folës ndërkombëtarë dhe 11 ekspertë kombëtarë: Dan Cimpean, VilmaTomco, Ogerta Koruti, Almerindo Graziano, Volha Litvinets, JustinNovak, Stefan Tanase, Andrei Bozeanu, Dorin Nedelcu, Laura Thaqi, Eralda Caushaj, Paweł Srokosz, Naim Isufi, Hergis Jica, Lawrence Rogers, Fatjon Kadillari, Rexhion Qafa, Saimir Kapllani, Lorin Baxhaku, Ergis Gaxho, Klorenta Pashaj, të cilët ndanë ekspertizën e tyre me 300+ pjesëmarrës online dhe më shumë se 70 pjesëmarrës unik në ditë.

Dita e fundit e akademisë ishte një sukses i vërtetë dhe një provë, që kapacitetet profesionale të ekspertëve shqiptarë dhe studentëve të rinj të talentuar po rriten vit pas viti, së bashku me Albanian CyberAcademy. Fituesit e "AKCESK 2021 CYBER EXERCISE" ishin oficerët e sigurisë nga Union Bank Albania, FED Invest dhe studenti red-teamer Franko Janku.



4. **AKCESK lancon iniciativën e "Pilotimit të Udhëzimeve për Mbrotjen e Fëmijëve në Internet (CoP) në Nivel Kombëtar"**

Autoriteti Kombëtar për CESK në partneritet me International Telecommunication Union lancuan iniciativën e "Pilotimit të Udhëzimeve për Mbrotjen e Fëmijëve në Internet (COP) në nivel kombëtar".

Ofruesit e Shërbimit të Internetit shprehën gadishmërinë e tyre për të kontribuar në arritjen e objektivave të përbashkët me qëllim rritjen e nivelit të sigurisë së fëmijëve dhe të rinjve në ekosistemin kibernetik. Gjithashtu, gjatë takimit u prezantua Moduli i Raportimit ne funksion te Platformes per bllokimin e aksesit te faqeve me permbajtje te palijgshme, realizimi i te cilit u mundesua nga Ambasada e Shteteve të Bashkuara në Tiranë.

5. Cyber Camp 2021

Autoriteti Kombëtar për Çertifikimin Elektronik dhe Sigurinë Kibernetike në bashkëpunim me Këshillin e Europës, Raiffeisen Invest dhe Universiteti Katolik "Zoja e Këshillit të Mirë" organizojne ne datat 6-8 Dhjetor aktivitetin inovativ "Cyber Camp Albania" prane Movenpick Hotel, Gjiri i Lalzit.

Qëllimi i Cyber Camp është krijimi i një mjedisi te sigurt per femijet e te rinjte, nepermjet bashkepunimit te ngushte institucional, ndergjegjesimit dhe ngritjes se kapaciteteve profesionale dhe teknike.

Në fjalën e hapjes, Ministri i Mbrojtjes Z.Peleshi, Ambasadori i OSBE në Shqipëri Z. Del Monaco, përfaqësues të Këshillit të Europës e Ministrisë së Arsimit, theksuan rëndësinë e bashkëpunimit për ndërtimin e një shoqërie të mbrojtur dhe të zhvilluar kibernetikisht.

Rezultatet e pritshme të këtij eventi janë në përputhje të plotë me shtyllat e Strategjisë Kombëtare për Sigurinë Kibernetike dhe në linjë me prioritet e Qeverisë Shqiptare.

Aktivitete për Ngritje Kapacitetesh

1. Aktiviteti "Cyber Health"

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike organizoi aktivitetin 5-ditor "Cyber Health" me përfaqësues të sektorit publik dhe privattë shëndetësisë.

Qëllimi i këtij aktiviteti është rritja e ndërgjegjësimit për ndërtimin e një shoqërie të zhvilluar digjitale, të mbrojtur kibernetikisht dhe të pajisur me njohuritë e nevojshme për të maksimizuar përfitimet dhe minimizuar rreziqet.

2. Aktiviteti "Financial Cyber Drill".

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, në përmbushje të detyrave funksionale dhe objektivave të "Strategjisë Kombëtare për Sigurinë Kibernetike" , në bashkëpunim me Shoqatën Shqiptare të Bankave (AAB) Albanian Association of Banks (Shoqata Shqiptare e Bankave), organizuan aktivitetin 2-ditor, ne datat 17- 18 Nëntor 2021, "Financial Cyber Drill".

Qëllimi i aktivitetit ishte ngritja e kapaciteteve të sektorit financiar, si një nga sektorët më sensitivë në nivel kombëtar.

3. Realizimi dhe publikimi i broshurave

Autoriteti Kombëtar për Certifikimin Eletronik dhe Sigurinë Kibernetike ka realizuar në bashkëpunim me RISI Albania 4 broshura për:

1. Siguria Kibernetike në Sektorin e Energjisë
2. Siguria Kibernetike në Sektorin Financiar
3. Siguria Kibernetike në ndërmarrjet e vogla e të mesme
4. Siguria Kibernetike në shëndetësi

Materiale promovuese

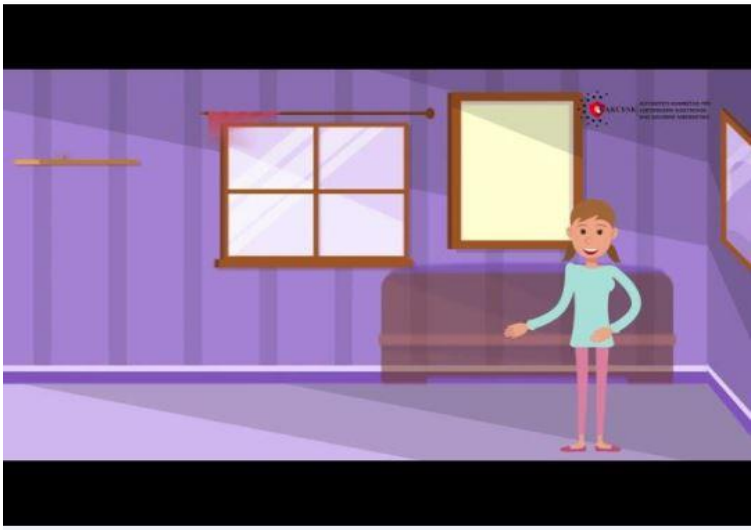
Përgjatë vitit 2021 në zbatim të planit të komunikimit të sektorit u krye realizimi dhe publikimi në rrjetet sociale te Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike i 4 videove promovuese për ndërgjegjësimin e komunitetit për rritjen e nivelit të sigurisë kibernetike.

Monitoro aksesin e fëmijës tend në internet

Aplikoni CYBER INSURANCE

Mbroni privatësinë tuaj online

Mendohuni mirë para se të postoni diçka online!
Mbroni privatësinë tuaj në hapsirën kibernetike!
.
#cybersecurity #onlinesafety #cybercrime #thinkcyber
.



Mbroni privatesine tuaj online!
youtube.com

Udhëzime për industrinë e mbrojtjes së fëmijëve në internet

Protect your CHILD and Be aware of what he/she is accessing on the Internet!
.
.
"This video has been developed as part of a collaboration agreement with the International Telecommunication Union within the context of ITU's global programming on child online protection."
.

Udhezime per industrine e mbrojtjes se femijeve ne Internet!
youtube.com

Buletinet e sigurisë kibernetike

Çdo muaj AKCESK publikon buletinin e sigurisë kibernetike me lajme dhe eventet kryesore të zhvilluara ose organizuara nga Autoriteti.

Janar 2022

Shkurt 2022

Mars 2022

Prill 2022

Maj 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Maj 2021

PREZANTIMI I "PORTALIT TË SINJALIZIMIT TË AKCESK"

Autoriteti Kombëtar për CESK në vijim të takimeve për mbrojtjen e fëmijëve në internet, si një nga objektivat e **"Strategjisë Kombëtare për Sigurinë Kibernetike"**, organizoi në datë 27 Maj 2021, takimin konsultativ, me qëllim prezantimin e ndërveprimit të aktorëve pjesëmarrës me **"Portalin e Sinjalizimit të AKCESK"**.

Gjatë takimit, theksi u vendos në forcimin e koordinimit ndërinstitucional për trajtimin me efektivitet të rasteve të raportuara dhe ngjitjen e problematikave të fëmijëve dhe të rinjve në internet, në lidhje me abuzimet seksuale online dhe elementët kontaminues që propagandojnë mbi radikalizimin dhe ekstremizmin e dhunshëm online.

Si të sigurohen cyber-physical supply chains?

Shkëmbimi i fushave dixhitale dhe fizike është një pjesë qendrore e transformimit dixhital që po kalojmë si pjesë e revolucionit të 4-të industrial. Këto sisteme fizike-kibernetike kombinojnë llogaritjen, rrjetëzimin dhe procesët fizike. Sistemet kibernetike zakonisht paraqesin një numër sfidash nga perspektiva e sigurisë kibernetike, duke përfshirë:

- Natyra e shpërndarë e kontrollit dhe menaxhimit të sistemeve kiber-fizike e bën të vështirë sigurimin efektiv të sistemit
- Shpejtësia dhe rrjedhshmëria e leximeve dhe statusi i sistemit mund të krijojnë dyshime
- Ato mund të përfshijnë loops kontrolli në kohë reale me kërkesa specifike të performancës
- Ato mund të përhapen gjeografikisht në një zonë të madhe, me përbërës lokacione që nuk kanë siguri fizike

https://cybernews.com/security/how-to-secure-cyber-physical-supply-chains/

Raport: Si i përdorin kriminelët kibernetikë çelësat API

Studiuesit kanë zbuluar se kriminelët kibernetikë janë në gjendje të abuzojnë me çelësat e shkëmbimit të kriptomonedhave API dhe të vjedhin kriptomonedhat nga llogaritë e viktimave pa u dhënë të drejta tërheqjeje. Në të njëjtën kohë, më shumë se $ 1,000,000 në kriptovaluta po mbahen në llogari të cilat kanë çelësat e tyre API të eksponuar në depot e kodit publik. Teknikat e përdorura nga kriminelët në internet:

- Bërja e 'sell walls'
- Rritja e çmimeve

Si të mbrojnë çelësat tuaj API:

- Bëni listë të bardhë adresën tuaj IP.
- Trajtoni çelësat tuaj API si çelësin privat të portofolit tuaj të kriptomonedhës

https://cybernews.com/security/report-how-cybercriminals-abuse-api-keys-to-steal-millions/

Sulmet DDoS arrijnë nivele rekord

Më shumë se **10 milion sulme** ndodhën vitin e kaluar-dhe akoma me shumë po ndodhin në 2021.

Sulmet nga kriminelët kibernetikë ndryshojnë shumë, nga sulmet duke përdorur teknika të phishing të akuzuara deri te DDoS. Dhe ndërsa kjo e fundit është më pak në qendër të vëmendjes kundrejt kaosit që mund të shkaktojë e para, kjo nuk do të thotë që ato nuk janë kritike.

Ne jemi ende në gjysmën e vitit, por tashmë nivelet e sulmeve DDoS gjatë vitit 2021 duket se po mposhtin edhe rekordet e tarta që janë paré në 12 muajt e mëparshëm. Aktorët e kërcënimit filluan afërsisht 2.9 milion sulme DDoS në tremujorin e parë të 2021, një rritje prej 31% nga e njëjta kohë në vitin 2020.

https://cybernews.com/security/ddos-attacks-reach-record-levels/

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Qershor 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Qershor 2021

Prania e OSBE-së në Shqipëri zhvillon workshop për "Parandalimi dhe hetimi i krimeve kibernetike"

Drejtori i Përgjithshëm i Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, **Vilma Tomco** mori pjesë në workshopin, "Parandalimi dhe Hetimi i Krimeve Kibernetike" më datën 29 Qershor 2021 për të mbështetur përpjekjet e vendit në luftën kundër krimit kibernetik, të organizuar nga Prezenca e OSBE-së në Shqipëri.

Gjatë workshop-it eksperti të fushës u njohën mbi zhvillimet e fundit në parandalimin e krimit kibernetik. Workshop u përqendrua gjithashtu në shkëmbimin e përvojave midis agencive të zbatimit të ligjit në rajon, duke siguruar një forum për oficerët e policisë, të akredituar në Tiranë, për të ofruar përvojat e tyre në lëvizshmin e hetimeve të krimeve kibernetike të iniciuara nga autoritetet e tyre përkatëse.

Raportimi i situatës mbi sulmet FLUBOT

Ky raport ofron një azhurnim të patcheve përsa i përket sulmeve që po përfaqsojnë dhe zgjerohen shpejtë, të malware-s së Flubot Android në Evropë, që nga fillimi i vitit 2021. Raporti bazohet në burime të hapura (Open Sources) për incidentet e Flubot, si raportohet në Shtete të ndryshme anëtare.

Malware-i Android i njohur si **FluBot**, po vazhdon të zgjerohet me shpejtësi në një numër në rritje të Vendet evropiane. Flubot vjedh fjalëkalimet dhe informacionin e hyrjes në llogaritë tuaja personale, detajet personale, dhe informacionin bankar. Informacioni përdoret për të bërë pagesa nga llogaritë e rrezikuara si dhe për vjedhjet e identitetit në internet. Flubot gjithashtu u dërgon mesazhe SMS viktimave të reja dhe përhapet vetë më tej. E gjithë kjo bëhet pa dijeninë e përdoruesve.

https://cesk.gov.al/Publikime/2021/Raport%20%26situates%20ne%20sulmet%20FLUBOT.pdf

ALBANIAN CYBER ACADEMY EDICIONI 5

Albanian Cyber Academy
5-th Edition

21
10 International speakers, 11 local experts

300+ participants in 1 week,
57% WOMEN

AKCESK 2021 CYBER EXERCISE

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Korrik 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Korrik 2021

KONFERENCA RAJONALE TELEKOMUNIKACIONI DHE SIGURIA E INFORMACIONIT

Drejtori i Përgjithshëm i Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, **Vilma Tomco** ishte një nga panelistet e konferencës rajonale "Telekomunikacioni dhe Siguria e Informacionit" , e organizuar nga Ballkan Youth Council, e cila u mbajt në datën 24 Korrik 2021, ne Hotel Rogner Tirana. Gjatë konferencës eksperte të fushës ndanë mendime dhe sugjerime mbi zhvillimet e fundit lidhur me sigurinë kibernetike.

Microsoft siguron RiskIQ ndërkohë që kërcënimi nga ransomware intensifikohet

Microsoft po merr zyrtarisht RiskIQ, një shitës softuerësh të sigurisë. RiskIQ siguron mjete menaxhimi dhe mbledhje të inteligjencës kundër kërcënimeve nga një game e gjerë sulmesh kibernetike në shërbimet cloud të Microsoft-it, AWS, etj. Ndërsa Microsoft nuk e ka vlerësuar marrëveshjen, Bloomberg raportoi se kompania thuhet se po paguan më shumë se 500 milion dollarë për RiskIQ.

Softueri RiskIQ i bazuar në cloud zbulon çështje të sigurisë në rrjete dhe pajisje. Kompania liston Box, Shërbimin Postar të SHBA, BMW, Facebook dhe American Express si klientë. RiskIQ u themelua fillimisht në 2009 dhe gradualisht është bërë një lojtar i rëndësishëm në analizimin e kërcënimeve të sigurisë.

https://www.theverge.com/22573778/microsoft-riskiq-acquisition-deal-cybersecurity-ransomware-security

Kina harton një plan të ri Për industrinë e sigurisë kibernetike

Ministria e Industrisë dhe Teknologjisë së Informacionit ka hartuar një projekt-plan veprimi tre-vjeçar për zhvillimin e industrisë së Sigurisë Kibernetike të vendit, duke vlerësuar se sektori mund të ketë vlerë më shumë se 250 miliardë juanë (38.6 miliardë dollarë) deri në vitin 2023.

Drafti vjen pasi autoritetet kinezë shtojnë përpjekjet për të hartuar rregullore për të menaxhuar më mirë rrjedhjen e të dhënave, transferimin e të dhënave dhe privatësinë e të dhënave personale.

https://www.reuters.com/world/china/china-drafts-new-cyber-security-industry-plan-2021-07-12/?utm_source=pocket_mylist

RAPORTOHET SE HAKERAT RUS SULMUAN SISTEMET KOMPJUTERIKE GOP

Hakerat rusë në bashkëpunim me grupin Cozy Bear fshihen pas një sulmi javën e kaluar në Synnex, i cili është një kontraktor që ofron shërbime IT për Komitetin Kombëtar Republikan (RNC). Sulmi mund të ketë eksponuar informacione te organizatës.

Në një deklaratë të lëshuar më 6 korrik, Synnex konfirmoi më tej "se është në dijeni të disa rasteve kur aktorët e jashtëm janë përpjekur të gjenë gaoje, përmes Synnex, në aplikacionet e klientëve brenda mjedisit cloud të Microsoft." Kompania pretendon se po shqyrton sulmin së bashku me Microsoft dhe me një firmë të sigurisë së palëve të treta. Manipulimi i softuerit të ndërmarrjes që ndërvepron me cloud të Microsoft -it në vend që të shkojë pas produkteve Azure ose Office, sidan dorëzëndrejt disa ngjashmëri me sulmin e SolarWinds në vitin 2020.

https://www.theverge.com/2021/7/6/22565779/rnc-breach-russian-hackers-cozy-bear

AGJËNCIA E UDHËTIMEVE CWT PËRBALLET ME NJË DËM PREJ 4.5MS SI PASOJË E NJË SULMI KIBERNETIK

CWT, një agjenci udhëtimi e korporatave me klientelë globale, mund të jetë përballur me pagesën prej 4.5 milion dollarësh për hakerat anonim pas një sulmi ransomware.

https://threatpost.com/cwt-travel-agency-ransom-cyberattack-report/157911/

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Gusht 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Gusht 2021

SULMI KIBERNETIK NDAJ TË DHËNAVE TË VAKSINËS SË COVID-19

Dokumentet rregullatore në lidhje me vaksinën Covid-19 që po zhvillon Pfizer u "aksesuan" në mënyrë të paligjshme" pas një sulmi kibernetik ndaj rregullatorit të llaqeve të Evropës, është shprehur firma bioteknologjike BioNTech.

BioNTech tha: "Sot, ne u informuam nga Agjencia Evropiane e Barnave se agjencia i ishte nënshtruar një sulmi kibernetik dhe se disa dokumente që lidhen me paraqitjen rregullatore për kandidatin e vaksinës Pfizer dhe BioNTech për COVID-19, ishin aksesuar në mënyrë të paligjshme."

Ai shtoi se "asnjë sistem BioNTech ose Pfizer nuk është shkelur në lidhje me këtë incident dhe ne nuk jemi në dijeni të aksesit të të dhënave personale të pjesëmarrësve në studim."

https://www.msn.com/en-gb/news/world/covid-19-vaccine-data-unlawfully-accessed-in-cyberattack-ema-regulator/ar-BB1jMMQC

Hakerët vjedhin 600 milionë dollarë në kriptomonedhë

Hakerët kanë vjedhur rreth 600 milion dollarë (433 milion £) në atë që duket të jetë një nga grabitjet më të mëdha të kriptomonedhës të ndodhur ndonjëherë.

Faqja Blockchain Poly Network u shpreh se hakerat kishin shfrytëzuar një dobësi në sistemin e tyre dhe kishin marrë mijëra token dixhital si; është Ether.

Në një postim në Twitter, ajo u bëri thirrje sulmuesve të "krijojnë komunikim dhe të kthejnë asetet e hakuara".

Disa ose pas hakimit, sulmuesi filloi të kthejë fondet - së pari në sasi të vogla dhe më pas në miliona.

https://www.bbc.com/news/business-58163917

T-Mobile pëson sulmin e pestë të të dhënave në 4 vite pasi hakerat vjedhin të dhënat e 100 milion përdoruesve

Një haker informoi VICE se ata vodhën të dhëna konfidenciale të 100 milion përdoruesve të T-Mobile. Shtësi në një bisedë me Motherboard, platforma e VICE e cila mbulon teknologjinë, zbuloi se të dhënat përmbajnë detaje si numrat e sigurimeve shoqërore, numrat e telefonit, emrat, adresat fizike, numrat unikë.

Sulmet kibernetike janë rritur gjatë pandemisë pasi blokimet e shkaktuara nga COVID-19 detyruan një adaptim të shpejtë të teknologjisë dixhitale. Shkeljet e të dhënave janë forma e dytë më e zakonshme e sulmeve kibernetike pasi informacioni i vjedhur merr një çmim fitimprurës në darkweb.

https://mcc.exchange/2021/08/16/t-mobile-suffers-fifth-data-breach-in-four-years-as-hackers-get-away-with-sensitive-data-of-100-million-users/

GJIGANTI ARSIMOR PEARSON GJOBITET ME 1 MILION DOLLARË PËR NËNVLERËSIMIN E RËNDËSISË SË SHKELJES SË TË DHËNAVE

Komisioni Amerikan i Letrave me Vlerë (SEC) njoftoi sot se Pearson, një kompani britanike e botimeve dhe shërbimeve arsimore ndërkombëtare, ka ngjidhur akuzat për mos ndihmesën gjatë procesit të zbulimit për një shkelje të të dhënave 2018 të zbuluar në Mars 2019.

Pearson pranoi të paguajë një gjobë prej 1 milion dollarë për të zgjidhur akuzat "pa pranuar ose mohuar gjetjet" që u përpoq të fshihte dhe minimizonte shkeljen e të dhënave të vitit 2018 që çoi në vjedhjen e "të dhënave të studentëve dhe kredencialeve të identifikimit të administratorit të 13,000 shkollave, llogaritë e klientëve të rrezikit dhe universitetit" në Shtetet e Bashkuara.

https://www.bleepingcomputer.com/news/security/education-giant-pearson-fined-1m-for-downplaying-data-breach/?&web_view=true

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Shtator 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Shtator 2021

AUTORITETI KOMBËTAR PËR CESK MERR PJESË NË KONFERENCËN KUSHTUAR SIGURISË KIBERNETIKE BLED, SLLOVENI

Në datat 2 dhe 3 shtator, në kuadër të Presidencës sllovene të Këshillit të BE-së, u organizua konferenca kushtuar Sigurisë Kibernetike.

Shqipëria u përfaqësua nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, Ministria e Mbrojtjes si edhe përfaqësues të institucioneve të tjera.

Në panelin e sigurisë kibernetike në Ballkanin Perëndimor, **znj. Vilma Tomco** prezantoi arritjet dhe sfidat e fushës, si edhe nevojat e bashkëpunimit në nivel rajonal dhe ndërkombëtar.

"HACKTECH 2021"

Drejtori i Përgjithshëm i Autoritetit Kombëtar për CESK , mori pjesë në sesionin e parë të "HackTech 2021", e organizuar nga "Canadian Institute of Technology - CIT" në bashkëpunim me York University dhe i mbështetur nga UNICEF Albania e institucione të tjera.

AKCESK LANCON INICIATIVËN E "PILOTIMIT TË UDHËZIMEVE PËR MBROJTJEN E FËMIJËVE NË INTERNET (COP) NË NIVEL KOMBËTAR"

Autoriteti Kombëtar për CESK në partneritet me International Telecommunication Union lancuan iniciativën e "Pilotimit të Udhëzimeve për Mbrojtjen e Fëmijëve në Internet (COP) në nivel kombëtar".

Ofruesit e Shërbimit të Internetit shprehën gadishmërinë e tyre për të kontribuar në arritjen e objektivave të përbashkët me qëllim rritjen e nivelit të sigurisë së fëmijëve dhe të rinjve në ekosistemin kibernetik. Gjithashtu, gjatë takimit u prezantua Moduli i Raportimit ne funksion te Platformes per bllokimin e aksesit te faqeve me permbajtje te paligjshme, realizimi i te cilit u mundesua nga Ambasada e Shteteve te Bashkuara ne Tirane.

"SIGURIA KIBERNETIKE NË SEKTORIN FINANCIAR"

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike është institucioni kryesor për përmirësimin e ekosistemit lidhur me Sigurisë Kibernetike në Shqipëri.

Autoriteti me mbështetjen e Risi Albania ka hartuar një sërë botimesh mbi situatën e sektorëve të ndryshëm në vend. Një ndër to është dhe broshura "Siguria Kibernetike në Sektorin Financiar"

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Tetor 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Tetor 2021

AUTORITETI KOMBËTAR PËR CESK MERR PJESË NË SAMITIN DIGJITAL TË BALLKANIT PERËNDIMOR

Në datat 12-13 Tetor, u organizua samiti digjital "WESTERN BALKANS DIGITAL SUMMIT",
Shqipëria u përfaqësua nga drejtori i përgjithshëm i Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

Në panelin e bashkëpunimit midis qeverisë dhe industrisë në fushën e sigurisë kibernetike në Ballkanin Perëndimor, **znj. Vilma Tomco** prezantoi arritjet dhe sfidat e fushës, si edhe nevojat e bashkëpunimit në nivel rajonal.

TETORI, MUAJI EVROPIAN I SIGURISË KIBERNETIKE

Muaji Evropian i Sigurisë Kibernetike (ECSM) është fushata vjetore e Bashkimit Evropian kushtuar promovimit të sigurisë kibernetike midis qytetarëve dhe organizatave të BE-së dhe ofrimit të informacionit të përditësuar të sigurisë në internet përmes rritjes së ndërgjegjësimit.

Fushata ECSM koordinohet nga Agjencia e Bashkimit Evropian për Sigurinë Kibernetike (ENISA) dhe Komisioni Evropian, dhe mbështetet nga Shtetet Anëtare të BE-së dhe qindra partnerë nga Evropa dhe më gjerë.

TWITCH PËSON RRJEDHJE MASIVE TË TË DHËNAVE PËR SHKAK TË KONFIGURIMIT TË GABUAR TË SERVERIT

Platforma interaktive e transmetimit të drejtpërdrejtë Twitch pranoi një "shkelje" pasi një poster anonim në bordin e mesazheve 4chan zbuloi kodin e tij burimor, një konkurrent të papublikuar të Steam nga Amazon Game Studios, detajet e pagesave të krijuesve, kompletet e zhvillimit të softuerit të pronarit dhe mjete të tjera të brendshme.

Shërbimi në pronësi të Amazon tha se "po punon me urgjencë për të kuptuar shkallën e kësaj", duke shtuar se të dhënat u ekspozuan "për shkak të një gabimi në një ndryshim të konfigurimit të serverit Twitch që më pas u aksesua nga një palë e tretë me qëllim të keq".

KËTO SISTEME PO PËRBALLEN ME MILIARDA SULME ÇDO MUAJ NDËRSA HAKERAT PËRPIQEN TË HAMENDËSOJNË FJALËKALIMET

Studiuesit paralajmërojnë se kriminelët kibernetikë po bëhen më agresivë në përpjekjet e tyre për të hyrë në shërbimet RDP duke shfrytëzuar fjalëkalimet e dobëta të përdorura në rrjetet e ndërmarrjeve.

Rrjetet kompjuterike po bombardohen në mënyrë agresive me miliarda sulme të fjalëkalimeve të hamendësuara ndërsa kriminelët kibernetikë përpiqen të shfrytëzojnë rritjen e protokollit të desktopit në distancë (RDP) dhe shërbimeve të tjera cloud në mjediset e korporatave.

Studiuesit e sigurisë kibernetike në ESET zbuluan 55 miliardë përpjekje të reja për sulme me forcë brutale vetëm midis majit dhe gushtit 2021 – më shumë se dyfishi i 27 miliardë sulmeve të zbuluara midis janarit dhe prillit.

Hamendësimi i suksesshëm i fjalëkalimeve mund t'u sigurojë kriminelëve kibernetikë një rrugë të lehtë drejt rrjeteve dhe një rrugë që ata mund të përdorin për të nisur sulme të mëtejshme, duke përfshirë dërgimin e ransomware ose malware të tjerë.

Pasi aksesojnë rrjetin, ata do të përpiqen ta përdorin atë akses për të fituar leje shtesë dhe për të manipuluar, duke kryer veprime si çaktivizimi i shërbimeve të sigurisë në mënyrë që të mund të kryejnë më lehtë aktivitetet e tyre keqdashëse.

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Nëntor 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Nëntor 2021

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE ORGANIZON AKTIVITETIN "CYBER HEALTH"

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike organizoi aktivitetin 5-ditor "Cyber Health" me përfaqësues të sektorit publik dhe privat të shëndetësisë.

Qëllimi i këtij aktiviteti është rritja e ndërgjegjësimit për ndërtimin e një shoqërie të zhvilluar digjitale, të mbrojtur kibernetikisht dhe të pajisur me njohuritë e nevojshme për të maksimizuar përfitimet dhe minimizuar rreziqet.

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE ORGANIZON AKTIVITETIN "FINANCIAL CYBER DRILL"

Financial Cyber Drill 17-18 Nëntor 2021

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, në përmbushje të detyrave funksionale dhe objektivave të "Strategjisë Kombëtare për Sigurinë Kibernetike", në bashkëpunim me Shoqatën Shqiptare të Bankave (AAB) Albanian Association of Banks (Shoqata Shqiptare e Bankave), organizuan aktivitetin 2-ditor, ne datat 17- 18 Nëntor 2021, "Financial Cyber Drill".

Qëllimi i aktivitetit ishte ngritja e kapaciteteve të sektorit financiar, si një nga sektorët më sensitivë në nivel kombëtar.

AFTËSITË E REAGIMIT NDAJ INCIDENTEVE NË SEKTORIN E SHËNDETËSISË

SECTORAL CSIRT CAPABILITIES

Agjencia e Bashkimit Evropian për Sigurinë Kibernetike publikoi një analizë të gjendjes aktuale të zhvillimit të aftësive sektoriale CSIRT në sektorin e shëndetësisë që nga zbatimi i Direktivës NIS.

https://www.enisa.europa.eu/news/enisa-news/on-the-watch-for-incident-response-capabilities-in-the-health-sector

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Dhjetor 2021

Buletini i Lajmeve të Sigurisë Kibernetike

Dhjetor 2021

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE ORGANIZON AKTIVITETIN "CYBER CAMP"

Autoriteti Kombëtar për Çertifikimin Elektronik dhe Sigurinë Kibernetike në bashkëpunim me Këshillin e Europës, Raiffeisen Invest dhe Universiteti Katolik "Zoja e Këshillit të Mirë" organizojnë ne datat 6-8 Dhjetor aktivitetin inovativ "Cyber Camp Albania" prane Movenpick Hotel, Gjiri i Lalzit.

Qellimi i Cyber Camp është krijimi i një mjedisi te sigurt per femijet e te rinjte, nepermjet bashkepunimit te ngushte institucional, ndergjegjesimit dhe ngritjes se kapaciteteve profesionale dhe teknike.

Në fjalën e hapjes, Ministri i Mbrojtjes Z.Peleshi, Ambasadori i OSBE në Shqipëri Z. Del Monaco, përfaqësues të Këshillit të Europës e Ministrisë së Arsimit, theksuan rëndësinë e bashkëpunimit për ndërtimin e një shoqërie të mbrojtur dhe të zhvilluar kibernetikisht.

Rezultatet e pritshme të këtij eventi janë në përputhje të plotë me shtyllat e Strategjisë Kombëtare për Sigurinë Kibernetike dhe në linjë me prioritet e Qeverisë Shqiptare.

SULMI KIBERNETIK SPAR PREK MË SHUMË SE 300 DYQANE

Një sulm kibernetik ka goditur më shumë se 300 dyqane Spar në të gjithë veriun e Anglisë duke i detyruar të mbyllin dyert e tyre.

Sulmi kishte në shënjestër James Hall & Company në Preston, Lancashire, e cila operon sistemet e Spar dhe IT.

Dyqanet që mbeten të hapura, nuk kanë mundur të kryejnë pagesa me kartë duke operuar vetëm para në dorë.

Qendra Kombëtare e Sigurisë Kibernetike dhe Policia e Lancashire jane duk hetuar.

RANSOMWARE DHE TERRORIZMI: PËR PROFESIONISTËT E SIGURISË, KËRCËNIMI ËSHTË I BARABARTË

Venafi njoftoi rezultatet e një sondazhi global me më shumë se 1500 vendimmarrës të sigurisë së IT-së, i cili zbulon se 60% e profesionistëve të sigurisë besojnë se kërcënimet e ransomware duhet të kenë përparësi në të njëjtin nivel me terrorizmin.

60% of security professionals believe ransomware threats should be prioritized at the same level as terrorism.

Ransomware and terrorism: For security pros the threat is equal - Help Net Security

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

1.3. Sektori i Kontrollit

Sektori i Kontrollit ka këto përgjegjësi:

a) Auditon ofruesit e kualifikuar të shërbimit të besuar (OKSHB) dhe operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit (OIKI-OIRI), në lidhje me përmbushjen e kërkesave të sigurisë, të përcaktuara sipas legjislacionit në fuqi.
b) Kontrollon dokumentimin dhe implementimin e masave minimale të sigurisë, teknike dhe organizative, nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në përputhje me kuadrin ligjor në fuqi dhe standardet ndërkombëtare.
c) Përgatit, harton dhe dërgon për miratim pranë eprorit programet e auditit të OKSHB, OIRI dhe OIKI.
d) Menaxhon dokumentacionin e plotë të auditimeve të ofruesve të kualifikuar të shërbimit të besuar dhe operatorëve të infrastrukturave të rëndësishme dhe kritike të informacionit.
e) Menaxhon procesin e auditeve të OKSHB-ve dhe OIKI-OIRI.
f) Kontrollon dokumentacionin teknik të OKSHB, në mënyrë që ato të jenë të njëjta me dokumentacionin e dorëzuar pranë AKCESK.
g) Kontrollon që OKSHB të ketë kryer, në periudhat kohore të përcaktuara, auditimet e brendshme.
h) Kontrollon raportet e auditimit të brendshëm, shkeljet e sigurisë që janë evidentuar dhe nëse janë marrë masat e duhura për mënjanimin e tyre, pranë OKSHB dhe OIKIOIRI.
i) Kontrollon të dhënat mbi punonjësit e zonave të sigurta dhe integritetin e tyre, pranë ofruesit të kualifikuar të shërbimit të besuar.
j) Verifikon listat e certifikatave të kualifikuara për vlefshmërinë e tyre, pranë OKSHB.
k) Kontrollon dhe auditon menaxhimin e aksesit të kontrollit, bazës së të dhënave, gjenerimin e çelësave, gjenerimin e certifikatave, integritetin dhe sigurinë e sistemit IT, sistemit të shfuqizimit dhe pezullimit të certifikatave, sistemin e vulave kohore, të OKSHB.
l) Kryen rolin e audituesit të jashtëm (Organizma e Testimit dhe Konfirmimit) për OKSHB, në rastin kur nuk ka të tilla të regjistruara pranë AKCESK.
m) Siguron funksionimin dhe përditësimin e regjistrit elektronik për procedurat e kontrollit.
n) Propozon masa administrative në raste të evidentimit të shkeljeve ligjore, ndaj ofruesve të kualifikuar të shërbimeve të besuara dhe operatorëve të infrastrukturave të rëndësishme dhe kritike të informacionit.
o) Menaxhon të dhëna sensitive të zotëruesve të nënshkrimeve elektronike, të cilat verifikohen gjatë auditeve pranë ofruesve të kualifikuar të shërbimit të besuar, si dhe të dhënat sensitive të OIRI dhe OIKI.
p) Në përputhje me metodologjinë për evidentimin e infrastrukturave kritike dhe të rëndësishme, propozon nismën për rishikimin e listës se tyre.
q) Menaxhon të dhëna statistikore mbi numrin e certifikatave të kualifikuara dhe transaksionet elektronike.

r) Menaxhon të dhëna statistikore të përdorimit të identifikimit elektronik dhe shërbimeve të besuara, në shërbimet publike elektronike.

Auditimi i Operatoreve të Infrastrukturave Kritike dhe të Rëndësishme të Informacionit.

Në përmbushje të detyrave funksionale, sektori i kontrollit gjatë vitit 2021, ka audituar operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me implementimin e masave minimale të sigurisë, teknike dhe organizative, nga këto operatorë, në përputhje me kuadrin ligjor në fuqi dhe standardet ndërkombëtare.
Konkretisht gjatë vitit 2021, Sektori i Kontrollit ka audituar, me metodën (onsite) vajtje në vend, operatorët e infrastrukturave kritike dhe te rëndësishme si mëposhtëm:

Infrastrukturat kritike:

1. AKSHI
2. Tirana Bank
3. Union Bank
4. Iute Credit
5. DPSHTR
6. OSHE
7. Autoriteti Portual Durrës
8. Alpha Bank

Infrastruktura te rëndësishme

1. Eurosig Sh.a
2. Fondi Besa
3. Albsig sh.a

Me qellim identifikimin e infrastrukturave të reja, kritike dhe të rëndësishme të informacionit, sektori kontrollit ka nisur procesin e identifikimit të operatoreve potencial në sektorin e shëndetësisë dhe në sektorin e energjisë.

Auditimi i Ofruesve të Kualifikuar të Shërbimit të Besuar (OKSHB)

Në përmbushje të detyrave funksionale sektori i kontrollit gjatë vitit 2021, ka audituar Ofruesit e Kualifikuar të shërbimit të besuar (OSHB), që operojnë në Republikën e Shqipërisë në zbatim të kuadrit ligjor përkatës. OKSHB ka detyrimin te raportoje periodikisht pranë AKCESK.

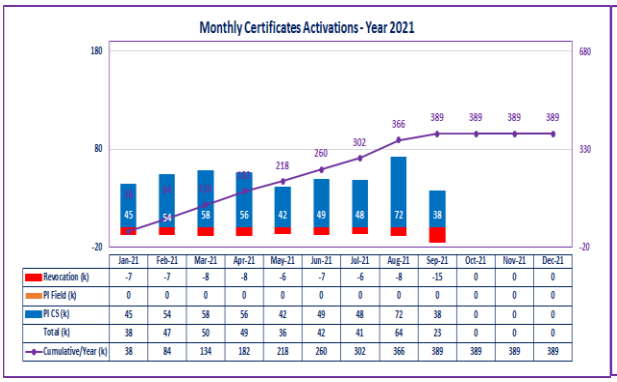
Gjatë vitit 2021, Sektori i Kontrolli ka mbikëqyrur veprimtarinë e OKSHB ALEAT në 82 zyrat e regjistrimit dhe shpërndarjes së certifikatave të kualifikuara në Republikën e Shqipërisë.

OKSHB ALEAT

OKSHB ALEAT gjatë vitit 2021 ka realizuar veprimtarinë si më poshtë:

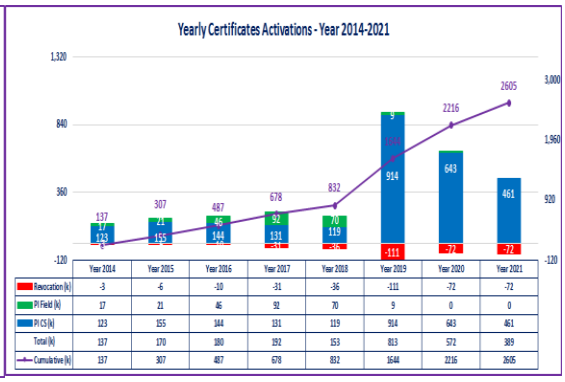
Pajisja me E-Certifikata

Procesi i pajisjes me e-Certifikata në Zyrat Qendrore të Aleat vazhdon që prej 1 Janar 2014. Pajisja me e-Certifikata gjithashtu përformohet në zyrat e Aleat, në 12 qarqe të Shqipërisë. Letërnjoftimet e-ID të certifikuara paraqiten në grafikët e mëposhtëm për vitin 2014 deri më 2021, së bashku me një raport mujor për vitin 2021. Aleat ka bërë të mundur që deri në fund të Dhjetorit 2021, të aktivizohen me këtë shërbim një total prej **2,679,869** letërnjoftime e-ID.



	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21
Revocation (k)	-7	-7	-8	-8	-6	-7	-6	-8	-15	0	0	0
PI Field (k)	0	0	0	0	0	0	0	0	0	0	0	0
PI CS (k)	45	54	58	56	42	49	48	72	38	0	0	0
Total (k)	38	47	50	49	36	42	41	64	23	0	0	0
Cumulative/Year (k)	38	84	134	182	218	260	302	366	389	389	389	389

Fig. 1: Aktivizimi i Letërnjoftimit E-ID për muaj (Jan - Dhjet 2021)

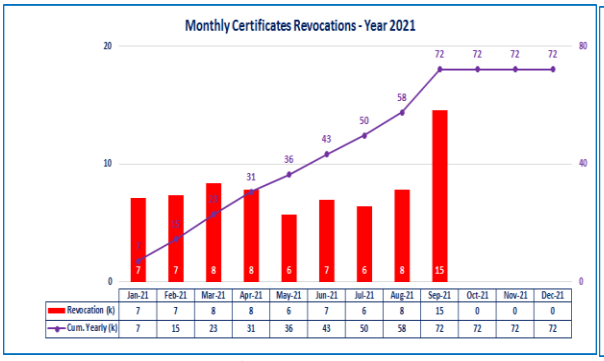


	Year 2014	Year 2015	Year 2016	Year 2017	Year 2018	Year 2019	Year 2020	Year 2021
Revocation (k)	-3	-6	-10	-31	-36	-111	-72	-72
PI Field (k)	17	21	46	92	70	9	0	0
PI CS (k)	123	155	144	131	119	914	643	461
Total (k)	137	170	180	192	153	813	572	389
Cumulative (k)	137	307	487	678	832	1644	2216	2605

Fig. 2: Aktivizimi i Letërnjoftimit E-ID sipas viteve dhe Kumulativi

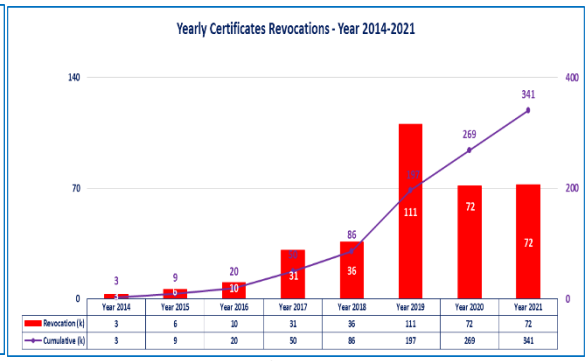
Lista e Shfuqizimit të e-Certifikatave

Një total prej **90,314** Certifikatash janë revokuar deri në fund të muajit Dhjetor 2021, duke përfaqësuar rreth **12%** të totalit të letërnjoftimeve ID të aktivizuara. Totali për muaj (Viti 2021) dhe totali për të gjithë periudhën (Viti 2014, 2015, 2016 , 2017, 2018, 2019, 2020, 2021 për referencë) Letërnjoftimeve eID të revokuara paraqitet në grafikun më poshtë.
Revokimi i certifikatave ndodh kryesisht për shkak të zëvendësimit të Letërnjoftimit ID, të pajisur me certifikatë (pas vitit 2014).



	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21
Revocation (k)	7	7	8	8	6	7	6	8	15	0	0	0
Cum. Yearly (k)	7	15	23	31	36	43	50	58	72	72	72	72

Fig. 3: Revokimi i Letërnjoftimit e-ID për muaj (Jan - Dhjet 2021)



	Year 2014	Year 2015	Year 2016	Year 2017	Year 2018	Year 2019	Year 2020	Year 2021
Revocation (k)	3	6	10	31	36	111	72	72
Cumulative (k)	3	9	20	50	86	197	269	341

Fig. 4: Revokimi i Letërnjoftimit e-ID sipas viteve dhe Kumulativi

Totali i e-Certifikatave
Aleat ka kryer me sukses aktivizimin me Certifikata Elektronike të rreth **464,143** (373,829 aktivizime – 90,314 revokime) të letërnjoftimeve ID deri në fund të Dhjetor 2021.

2,679,869 Letërnjoftimet ID të aktivizuara përmbajnë certifikata të vlefshme dhe përfaqësojnë rreth **76.6%** të Letërnjoftimeve ID.

Aktivitete të performuara përgjatë Tremujorit të Katërt / 2021

Zhvillimet në Sektorin Privat
Aktualisht, Aleat ka nënshkruar 11 (njëmbëdhjetë) marrëveshje për Projekte Pilot. Aktualisht 7 (shtatë) prej tyre operojnë Live me një total prej 70 degësh:

- Raiffeisen Bank (13 degë),
- OTP Bank (6 degë)
- Union Bank (3 degë),
- NOA (10 degë)
- Intesa Sanpaolo Bank (34 degë),
- Kredo Finance (3 degë)
- Austrian Institute of Excellence (1 degë).

Ndërkohë 4(katër) janë gati për të filluar: AADF, BKT, Posta Shqiptare dhe ACER Albania. Easy Pay, Fed Invest dhe Dhoma Kombëtare e Noterëve janë në statusin e pritjes.

Gjatë Tremujorit të Katërt të 2021, janë kryer rreth **27,102 transaksione**, duke arritur një total prej **237,603.000 transaksionesh** të suksesshme që nga lançimi i shërbimit në vitin 2016.

OKSHB AKSHI

OKSHB AKSHI gjatë vitit 2021 ka realizuar veprimtarinë si më poshtë:

a) 25 616 certifikata elektronike për subjektet private
b) 3 112 certifikata elektronike për administratën publike
c) 311 certifikata elektronike për doganierë dhe 235 certifikata për agjentët doganorë
d) 91 vula elektronike të gjeneruara për institucionet publike
e) 97 776 certifikata për projektin e fiskalizimit për subjektet private
f) 1 259 certifikata për projektin e fiskalizimit për institucionet publike
g) 3 753 certifikata për sistemin e-Receta

Gjatë vitit 2021 janë revokuar 239 certifikata elektronike. Prej tyre 90 janë certifikata elektronike të lëshuara për nëpunësit e administratës publike, 2 për nëpunës të sektorit privat, 119 certifikata elektronike për projektin e fiskalizimit, 27 certifikata elektronike për mjekë dhe 1 certifikatë për farmacist.

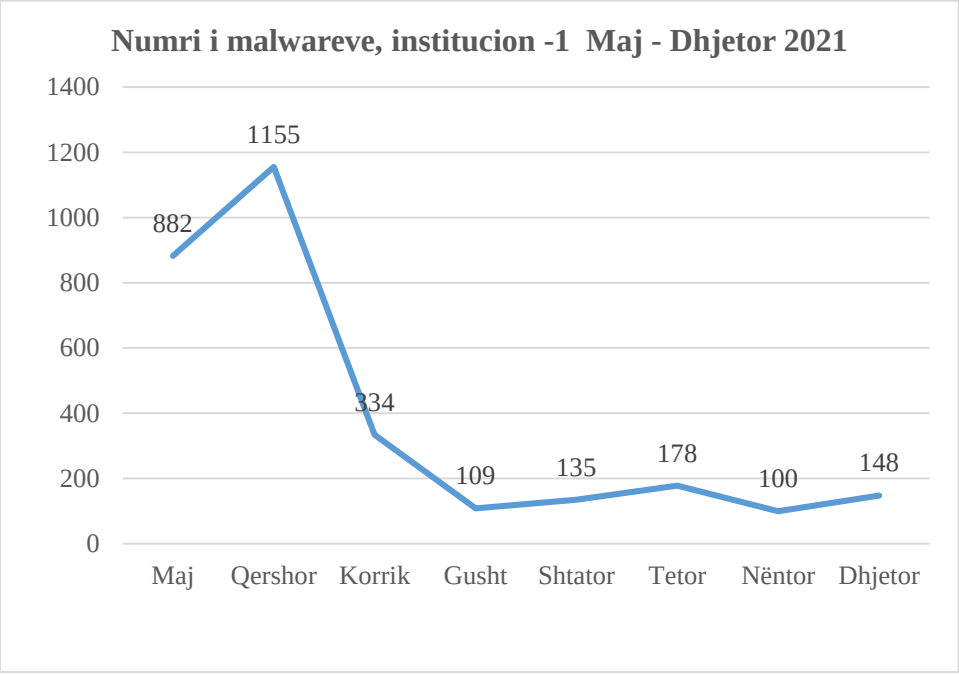
2. Drejtoria e AL-CSIRT

2.1. Sektori i monitorimit të incidenteve kibernetike

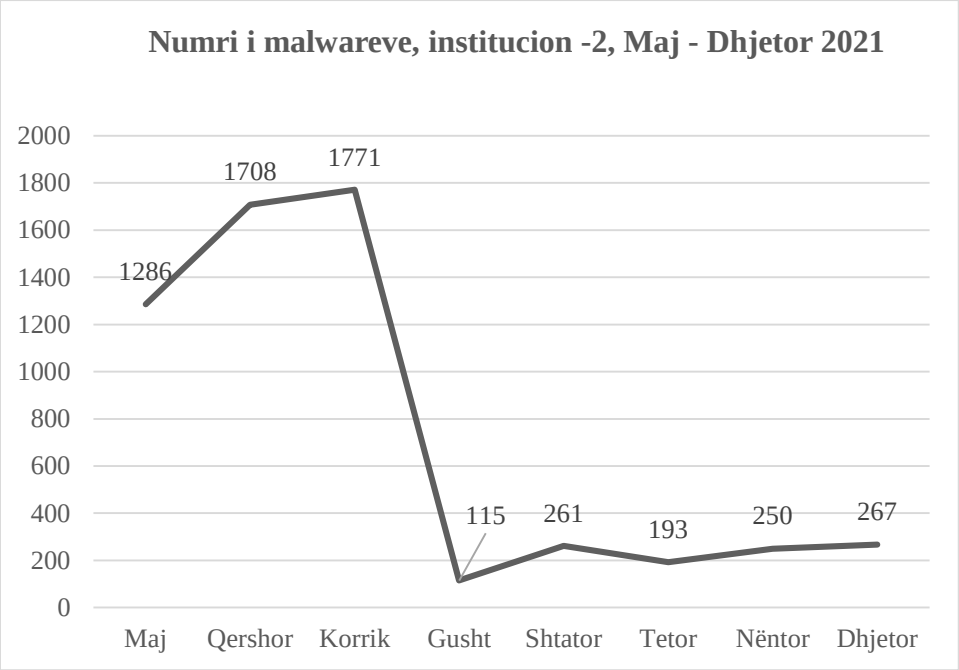
Në zbatim të VKM-së nr. 141, datë 22.02.2017, AKCESK administron dhe mirëmban sistemin unik on-line, për publikimin e faqeve të internetit me përmbajtje të paligjshme, ka dhënë suport për institucionet, për aksesimin e Portalit Online. Agjencia Shtetërore për Mbrojtjen e të Drejtave të Fëmijëve gjatë vitit 2021 ka raportuar në Portalin Online 72 faqe me përmbajtje të paligjshme të cilat janë evidentuar në rrjetet sociale dhe youtube.

Monitorimi i disa institucioneve shtetërore dhe Internet Service Provider që operojnë në Shqipëri të cilët gjenerojne malware me burim (source) Shqipërinë dhe me destinacion shtete të ndryshme, nëpërmjet informacionit që na vjen nga Shadow Server. Përpunimi i të dhënave të nxjerra nga ky monitorim si dhe hartimi i raportit. Si më poshtë jepen grafikët përkatës për çdo institucion dhe ISP duke i shprehur me institucion 1 dhe institucion 2, gjithashtu edhe ISP –të me, ISP 1 etj.

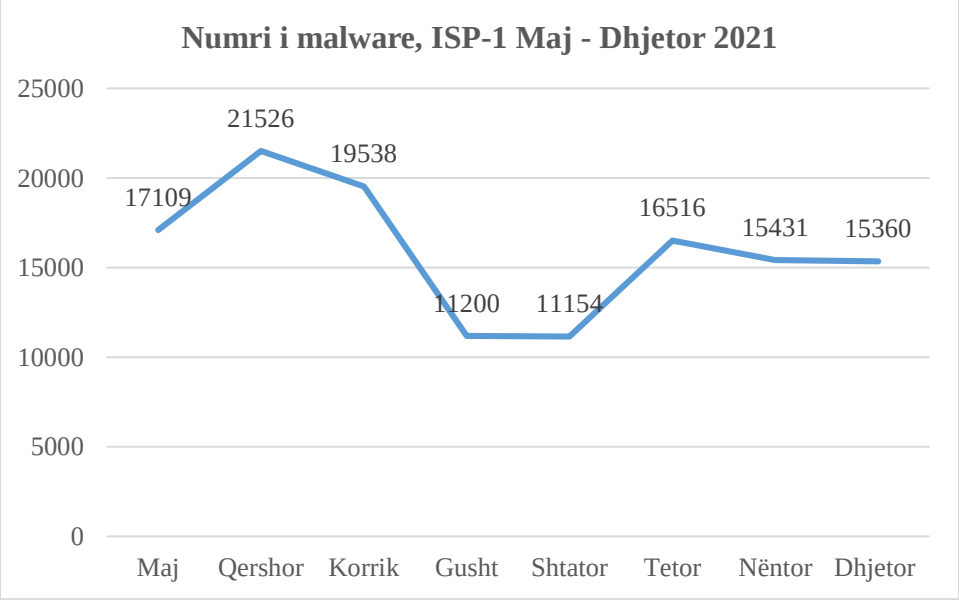
Institucioni -1



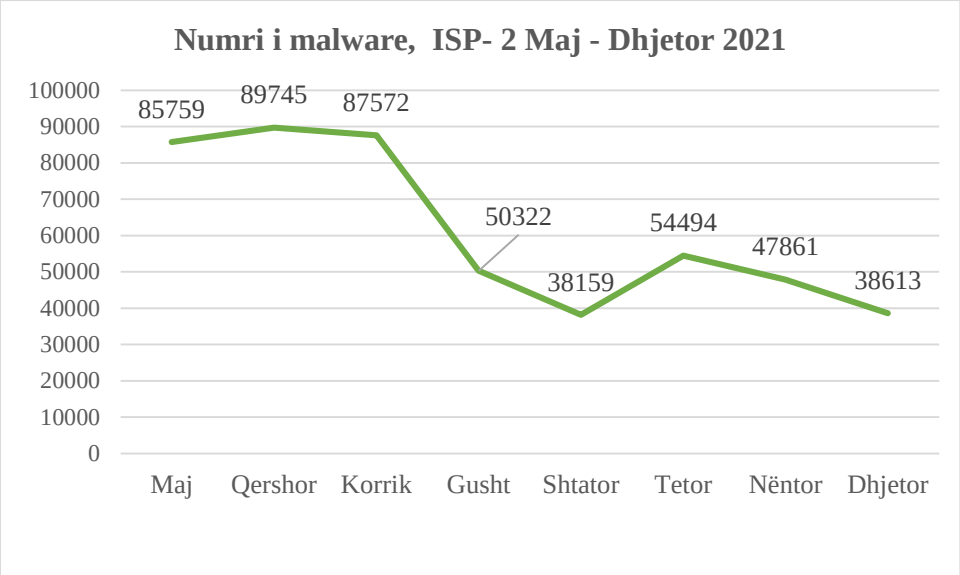
Institucioni -2



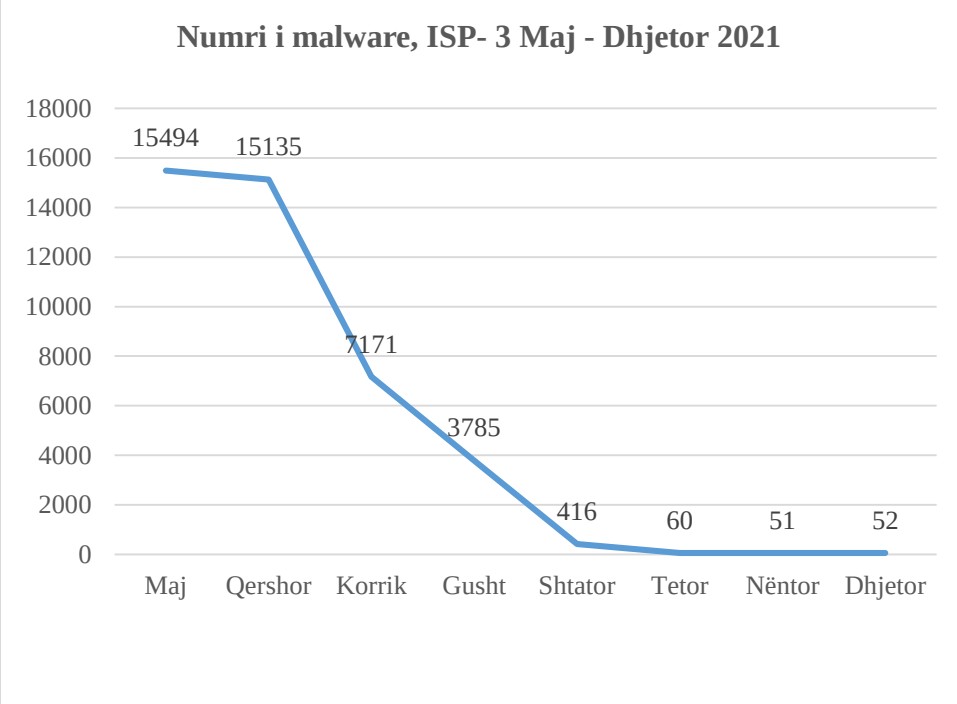
ISP -1



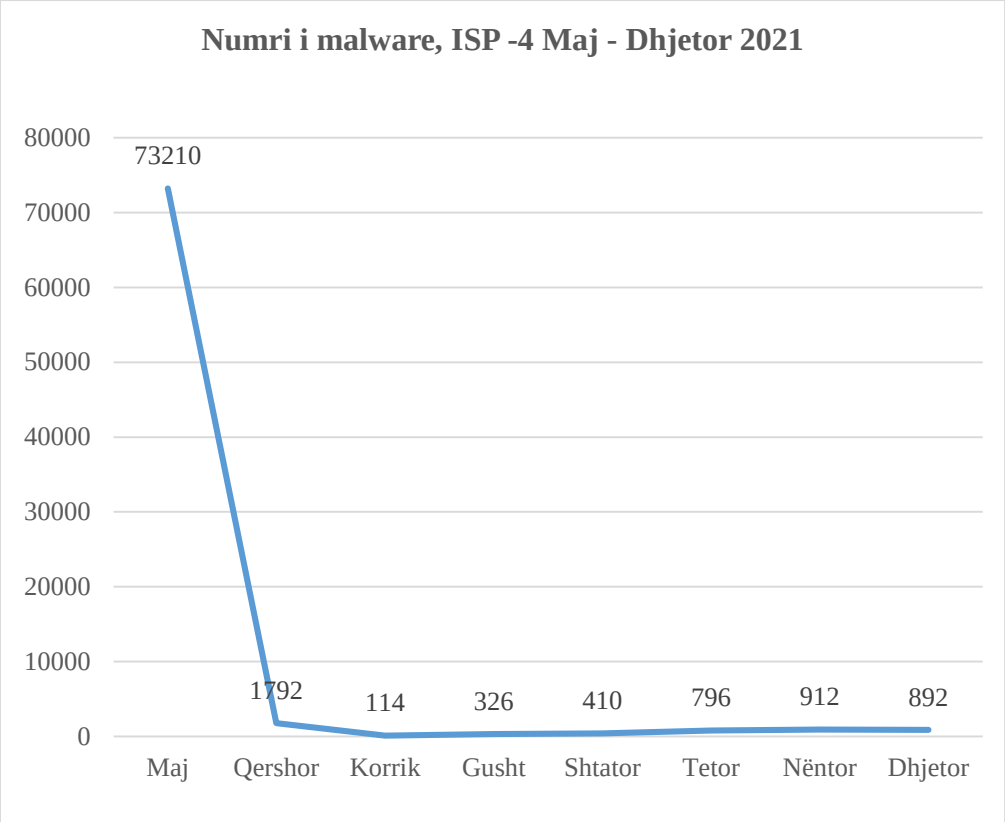
ISP -2


Numri i malware, ISP- 2 Maj - Dhjetor 2021
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
85759
89745
87572
50322
38159
54494
47861
38613
Maj
Qershor
Korrik
Gusht
Shtator
Tetor
Nëntor
Dhjetor

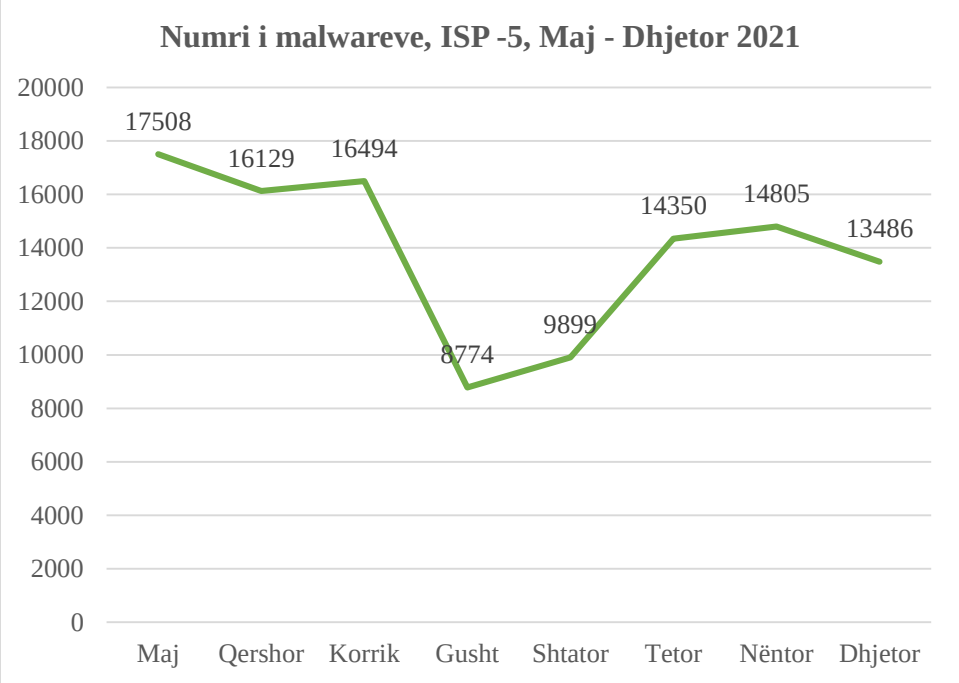
ISP -3


Numri i malware, ISP- 3 Maj - Dhjetor 2021
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
15494
15135
7171
3785
416
60
51
52
Maj
Qershor
Korrik
Gusht
Shtator
Tetor
Nëntor
Dhjetor

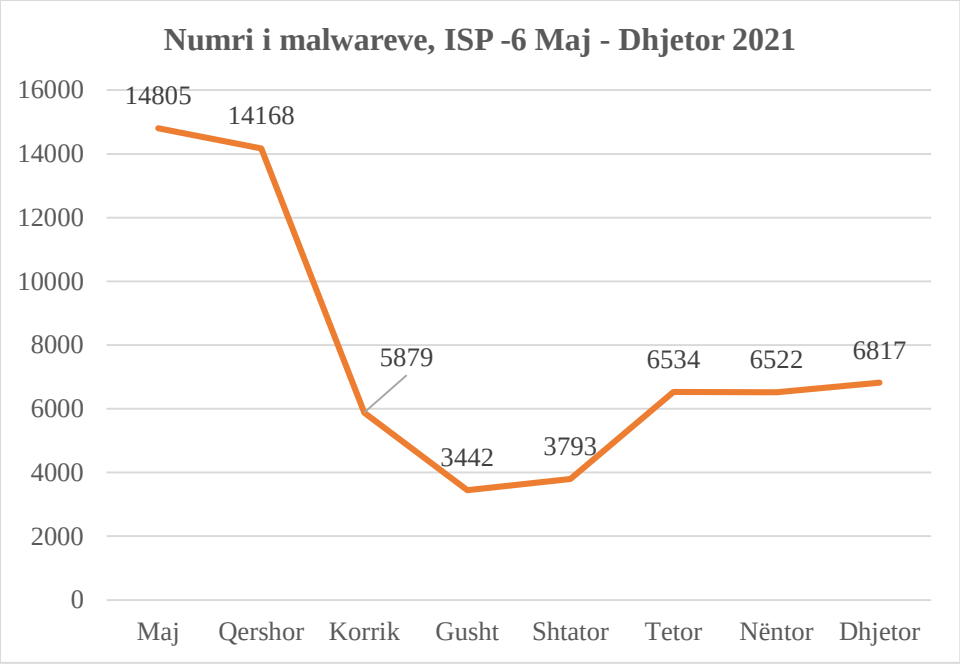
ISP -4


Numri i malware, ISP -4 Maj - Dhjetor 2021
80000
70000
60000
50000
40000
30000
20000
10000
0
73210
1792
114
326
410
796
912
892
Maj
Qershor
Korrik
Gusht
Shtator
Tetor
Nëntor
Dhjetor

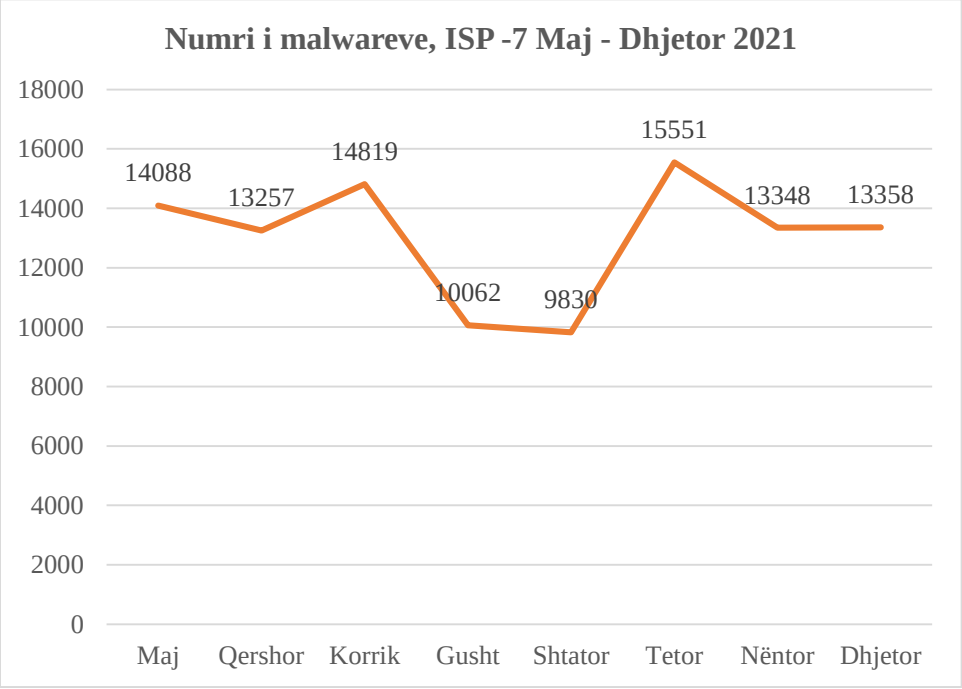
ISP -5


Numri i malwareve, ISP -5, Maj - Dhjetor 2021
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
17508
16129
16494
8774
9899
14350
14805
13486
Maj
Qershor
Korrik
Gusht
Shtator
Tetor
Nëntor
Dhjetor

ISP -6


Numri i malwareve, ISP -6 Maj - Dhjetor 2021
16000
14000
12000
10000
8000
6000
4000
2000
0
14805
14168
5879
3442
3793
6534
6522
6817
Maj
Qershor
Korrik
Gusht
Shtator
Tetor
Nëntor
Dhjetor

ISP -7


Numri i malwareve, ISP -7 Maj - Dhjetor 2021
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
14088
13257
14819
10062
9830
15551
13348
13358
Maj
Qershor
Korrik
Gusht
Shtator
Tetor
Nëntor
Dhjetor

1. Identifikimi dhe monitorimi i websiteve shtetërore të kompromet uar, njoftuar institucionet përaktëse.
2. Pjesëmarrja në webinare të organizuar nga Këshilli i Europës në kuadër të projektit iProceeds me tema:
   - **a.** Analizë e situatës mes CSIRT/LEA përmirësimin e procedurave dhe udhëzimeve për bashkëndarjen e informacionit nga CSIRT me autoritetet e drejtësisë penale në Shqipëri.
   - **b.** Workshop online mbi tendencat e krimit kibernetik dhe të sigurisë kibernetike si dhe për statistikat e drejtësisë penale në Shqipëri.

2.2. Sektori i menaxhimit të incidenteve kibernetike

Sektori i menaxhimit të incidenteve kibernetike ka këto përgjegjësi të përcaktuara në rregulloren e brendshme të institucionit:

- **a)** Realizimi i monitorimit të sistemit mbi raportimin dhe menaxhimin e incidenteve kibernetike, në Infrastrukturave Kritike dhe të Rëndësishme të teknologjisë së informacionit.
- **b)** Bashkërendimi i punës për zgjidhjen e incidenteve të sigurisë kibernetike me operatorët përgjegjës në fushën e sigurisë kibernetike kombëtare dhe ndërkombëtare.
- **c)** Kryerja e kërkimeve të vazhdueshme mbi zhvillimet në fushën e sigurisë kibernetike dhe rekomandon përditësime sigurie në rastin e konstatimeve të vulnerabiliteteve.
- **d)** Pjesëmarrja në grupe të ndryshme pune.
- **e)** Koordinimi i punës me sektorët e tjerë për te realizuar trajnime periodike për CSIRT-et sektoriale, me qellim rritjen e kapaciteteve profesionale të tyre.

- Gjatë vitit 2021 janë raportuar nga OIKI/OIRI apo dhe nëpër informacione të marra nëpërmjet partnerëve apo palëve të treta Incidentet Kibernetik si më poshtë:

a) Malicious Activity "Trickbot", Win32/Trickbot

Incidenti është trajtuar për eliminimin e aktivitetit të dëmshëm dhe futja e IP në blacklist.

U morën masa për bllokimin e këtyre ip keqdashëse. Kompania nga ku vjen aktiviteti i malicious IP (Ab-com/ Vodafone).

b) ASIG - DDoS attack

Incidenti është trajtuar nga Akshi dhe nuk është me prezent, por është dërguar nga operatori OIKI si raportim i ngjarjes së sigurisë. Si një masë shtesë për menaxhimin e këtij incidenti u është dërguar email CIRT/CSIRT'eve homologe për bllokimin e këtyre IP-ve.

c) CERT GIB - Phishing or Social Engineering

Është proceduar nga ana e sektorit të "Menaxhimit të Incidenteve" me një kërkesë zyrtare drejt AKEP për të bllokuar këto linqe: 109.104.151.11/ing, 109.104.151.11/abn nga ISP Ab-com (Vodafone) të cilat kanë qënë burimi i sulmeve.

d) Sistemi Qëndror Bankar (Banka Kombëtare Tregtare) - Phishing or Social Engineering

Është proceduar nga ana e sektorit të "Menaxhimit të Incidenteve" me një kërkesë zyrtare drejt AKEP për mbylljen e IP e cila gjeneron phishing domain.

Gjithashtu nga sektori i "Menaxhimit të Incidenteve" u është komunikuar me anë të sistemit të gjithë operatorëve të infrastrukturave OIRI/OIKI si informacion sensibilizues dhe paralajmërues, për marrjen e masave mbrojtëse/parandaluese nga sulmet e kësaj natyre. Gjithashtu u janë dërguar edhe rekomandime për sa i përket parandalimit dhe menaxhimit të këtyre sulmeve.

e) Netcraft (Ing Netherlands) - Phishing or Social Engineering

Është proceduar nga ana e sektorit të "Menaxhimit të Incidenteve" me analizimin e sulmi ku u konstatua se sulmi ishte akoma prezent dhe gjeneronte disa linqe të tjera "Phishing". IP nga ku gjeneroheshin këto sulme ishte [109.104.151.11] Është proceduar nga ana e sektorit të "Menaxhimit të Incidenteve" me një kërkesë zyrtare drejt AKEP për menaxhimin e këtij incidenti me ISP përkatëse, te cilat kane marrë masa të menjëhershëm për ndërprerjen e këtij aktiviteti.

f) incibe-cert (incidencias@incibe-cert.es) - Phishing or Social Engineering

Rasti është adresuar tek CERT Kombëtar i Republikës së Kosovës, tek palët relevante dhe është realizuar në kohën e duhur frenimi i aktivitetit me përmbajtje të paligjshme.

g) CERT SERB (CERT of the Spanish National Cybersecurity Institute (INCIBE-CERT))DDoS attack

Është proceduar nga ana e sektorit të "Menaxhimit të Incidenteve" me një kërkesë zyrtare drejt CERT Kombëtar të Serbisë për marrjen e logeve. Gjithashtu nga sektori i "Menaxhimit të Incidenteve" është proceduar me krijimin e rekomandimeve përkatëse si dhe procedurat për bllokimin e veprimeve keqdashëse të këtyre IP've.

Ekipi i Menaxhimit të Incidenteve në bashkëpunim edhe me sektorët e tjerë të AKCESK ka marrë të gjitha masat për reduktimin e impaktit të këtyre incidenteve në momentin e ndodhjes si dhe masa të tjera korrigjuese dhe ndërgjegjësuese në të gjithë operatorët për parandalimin e sulmeve të ngjashëm.

- Duke shfrytëzuar marrëveshjet e bashkëpunimit MoU me Cirt'et rajonale dhe ato ndërkombëtare është kryer komunikimin i vazhdueshëm me këto ekipe për bashkëpunim në incidentet e ndodhura dhe ato të mundshme të cilat kanë afektuar apo mund të afektojnë Operatoret e Infrastrukturave Kritike dhe të Rëndësishme në Republikën e Shqipërisë.

- Duke bashkëpunuar me partnerë ndërkombëtarë si:
  - Qualys

- EATM Cert
- Shadowserver

dhe me sektorët e tjerë të AKCESK (sektori i Kontrollit) janë prodhuar dhe publikuar në interval kohor (javor dhe 2-javor) të rekomandimeve si dhe vulnerabiliteteve të evidentuara të sistemeve TIK. Këto raporte përditësimi u janë dërguar OIKI dhe OIRI me anë të Sistemit të Monitorimit dhe Menaxhimit të Incidenteve si dhe nëpërmjet e-mailit zyrtar të institucionit për ata operatorë të cilët kanë hasur problem në aksesimin e sistemit.

Sektori i Menaxhimit të Incidenteve ka prodhuar dhe publikuar:

- Latest_VULNERABILITIES.CVS 12 raporte për 2021
- Shadow Server raporte ne sistem: 123
- Pulse Connect Secure.pdf date: 20.05.2021 15:28:39
- Rekomandime per Sulmet Phishing Akcesk.pdf date: 07:06:2021 13:25:15
- Kaseya VSA Supply-Chain Ransomware attach.pdf date: 08.07.2021 11:30:07
- Fortinet CVE-2018-13379.pdf date: 09.09.2021 16:46:40
- CVE-2021-38647.pdf date: 21.09.2021 09:48:29
- Avalanche-andromeda malware.pdf date: 30.09.2021 14:46:32
- Diwbadyo-cibfucjer.pdf date: 30.09.2021 14:46:32
- Necurs malware.pdf date: 30.09.2021 14:46:32
- Sality malware.pdf date: 30.09.2021 14:46:32
- Linux Ransomwares.pdf date: 02.11.2021 15:27:03
- Conti Ransomware.pdf date: 01.12.2021 10:47:08
- AKCESK Guidelines for responding to DDos attacks_Nov.2021.pdf date: 03.12.2021 14:11:50
- Log4j Vulnerability.pdf date: 20.12.2021 11:17:21
- Log4j vulnerability Update v.1.2.pdf date: 28.12.2021 15:29:38
- Mobile banking fraud (Mashtrimi permes mobile e-commerce) . pdf
  date: 27.01.2022 13:12:42

Pjesëmarrje në grupet e ndryshme të punës në dhënien e asistencës për kryerjen e detyrave për secilin sektor kryesisht në kryerjen e detyrave të auditit së bashku me Sektorin e Kontrollit.

Vlen te theksohet bashkëpunimi me të gjithë sektorët e AKCESK për mbajtjen e Statusit:

- "Accredited Member" nga Trusted Introducer ne 27 Maj 2020.
- "Fellow Member" nga FIRST (Forum for Incident Response Teams) 24 Shkurt 2020

3. Sektori i financës dhe shërbimeve mbështetëse

Për Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike buxheti i alokuar për vitin 2021 është 57,232 mijë lekë nga të cilat 40,998 mijë lekë Shpenzime Korrente dhe 4,000 mijë lekë Shpenzime Kapitale me financim të brendshëm.
Në vijim paraqesim më të detajuar realizimin e shpenzimeve sipas fondeve të alokuara:

Llogaria	Totali	Realizimi
600	31,664,000	25,016,000
601	3,939,000	4,573,000
602	17,529,000	11,260,000
605	0	149,000
606	100,000	0
231	4,000,000	0
Shuma	57,232,000	15,982,000

Fondi i Pagave dhe Sigurimeve Shoqërore (zërat 600+601) Shumat e alokuara për paga dhe sigurime shoqërore per vitin 2021 janë përkatësisht 31,664,000 lekë për artikullin 600 dhe 3,939,000lekë për artikullin 601. Dhe realizimi është përkatësisht 25,016,000 lekë për artikullin 600 dhe 4,573,000lekë për artikullin 601.

Fondi për shpenzime në mallra dhe shërbime (zëri 602) Shuma e alokuar për vitin 2021 për shpenzime operative është 17,529,000 lekë. Dhe realizimi për këtë artikull është 11,260,000 lekë.

Fondi i Veçantë (zëri 606) Shuma e alokuar për vitin 2021 për shpenzime për ndihma në fatkeqësi është 100,000 lekë. Dhe realizimi për këtë artikull është 0 lekë.

Fondi për Investime të brendshme (zërat 230+231), është miratuar në shumën 4,000,000 lekë në zërin 231. Dhe realizimi për këtë artikull është 0 lekë.

AKCESK në fillim të vitit 2020, konkretisht me Urdhrin e Kryeministrit Nr. 6, datë 16.01.2020 miratoi strukturën e re. Me strukturën e re u shtuan dhe 7 pozicione te reja dhe numri i planifikuar i stafit arriti në 24.

Gjatë vitit 2021 kemi bërë rekrutime të reja duke e shtuar numrin e stafit me 3 punonjës.