REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Informacion mbi implementimin e teknikave të nevojshme për bllokimin e platformës Tik Tok në Republikën e Shqipërisë

Adresa: Rruga “Papa Gjon Pali II” nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

Baza Ligjore

Bazuar në VKM nr. 151, datë 6 Mars 2025, "Për marrjen e masave të përkohshme për shmangien e ndikimeve negative të platformës online "Tik Tok", nenin 33 pika 3, gërma c, i ligjit nr. 25/2024 "Për Sigurinë Kibernetike", ligjin nr. 18/2017 "Për të drejtat dhe mbrojtjen e fëmijës", Ligjin nr. 124/2024 "Për mbrojtjen e të dhënave Personale", si edhe në Urdhrin e Përbashkët nr. 89, datë 07.03.2025 "Për miratimin e masave teknike dhe proceduriale për realizimin e ndërprerjes së përkohshme të aksesit në platformën online TikTok dhe detyrimin e sipërmarrësve të komunikimeve elektronike për zbatimin e tyre", Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK), në bashkëpunim me entet rregullatore të fushës u ngarkua për marrjen e masave të nevojshme teknike për të ndërprerë aksesin në platformën online "Tik Tok " në territorin e Republikës së Shqipërisë, për një afat prej 12 (dymbëdhjetë) muaj, me qëllim shmangien e ndikimeve negative dhe të problematikave sociale në tërësi deri në mundësimin nga ofruesi të instrumenteve teknike që rregullojnë aksesin e fëmijëve në këtë platformë.

Në zbatim të këtij vendimi AKSK në bashkëpunim me Autoritetin e Komunikimeve Elektronike dhe Postare (AKEP) nxorrën urdhrin e përbashkët nr. 89, datë 07.03.2025 "Për miratimin e masave teknike dhe proceduriale për realizimin e ndërprerjes së përkohshme të aksesit në platformën online Tik Tok dhe detyrimin e sipërmarrësve të komunikimeve elektronike për zbatimin e tyre", i cili përcakton hapat konkret që duhet të ndjekin institucionet për arritjen e këtij qëllimi.

Implementimi teknik

Në kuadër të zbatimit të këtyre masave AKSK ndërmori hapat e mëposhtme:

1. Ngritjen e një grupi teknik pranë AKSK-së i cili do të gjurmojë dhe gjejë DNS (Domain Name System), SNI (Server Name Indication) dhe IP (Internet Protocol) të cilat përdor platforma TikTok. Duke ditur që kjo platformë është dinamike dhe e ndryshon vazhdimisht qasjen e saj, gjurmimi i saj kryhet në mënyrë të përditshme.
2. Dërgimi i listës së DNS, SNI dhe IP drejt Autoritetit të Komunikimeve Elektronike dhe Postare (AKEP) për ti dërguar ato më pas drejt të gjitha kompanive të ofrimit të shërbimit të internetit në vendin tonë (numërohen mbi 250 të tilla), në mënyrë që t`i vendosin ato në listën e zezë « black list ».
   Ky bllokim ul aksesin e përdoruesve në platformën TikTok, por ka efikasitet deri në 20-25%, për shkak se kjo platformë përdor teknikat e avancuara CDN (Content Delivery Network) për shpërndarjen e trafikut. Kjo lloj teknologjie është dinamike dhe e bën të vështirë gjurmimin dhe më pas bllokimin e këtij trafiku për shkak se platforma ndryshon në mënyrë të vazhdueshme burimin e saj.
3. Dërgimin e kërkesës zyrtare drejt kompanive Google dhe Apple ku i kërkohet implementimi i teknikës mbështetur në bllokimin e vendndodhjes, të njohur si: « GeoLocation Country Block » për aplikacionin Tik Tok. Kjo do të shkaktojë mos

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

shfaqjen e aplikacionit përmes shkarkimit nga platformat App Store dhe Play Store të paisjeve telefonike mobile.

Kjo lloj mase do të bënte të papërdorshme përdorimin e Tik Tok përmes teknikës VPN VETËM për përdoruesit e rinj si edhe njëkohësisht do të bllokonte rifreskimet e vazhdueshme të Tik Tok, pavarësisht VPN-ve të instaluara në platformat e tyre, duke e bërë jo eficent TikTok.

Nëse kjo masë do të ishte efiçente për përdoruesit e telefonave të kompanisë Apple, nuk do të ishte plotësisht efiçente për përdoruesit e sistemeve Android, pasi kjo platformë të lejon të përdorësh burime të besueshme por edhe të pabesueshme që do të çonin në shmangien e këtij kufizimi.

AKSK është në komunikim të vazhdueshëm me kompanitë Google dhe Apple për të shtuar këtë atribut.

4. U dërgua kërkesë zyrtare shpërndarësve më të mëdhenj të trafikut CDN (Content Delivery Network) si Akamai, Fastly, CloudFlare, CDN77, AWS, Google për të mos lejuar trafikun TikTok në territorin e Shqipërisë. Deri më tani, Akamai dhe Fastly janë përgjigjur pozitivisht kërkesës sonë.
5. Qeveria Shqiptare është në komunikim të vazhdueshëm me kompaninë që ofron platformën TikTok në lidhje me marrjen e masave teknike për garantimin dhe mbrojtjen e fëmijëve në hapësirën online. Drejt kësaj kompanie është kërkuar marrja e masave për njohjen e gjuhës shqipe nga aplikacioni si edhe përfshirjen e filtrave të nevojshem për identifikimin e gjuhës se urrejtjes dhe bllokimin e përmbajtjes.
6. Të gjitha masat e përmendura më sipër janë efiçente deri në 40-45%. Vështirësi hasen kryesisht për bllokimin e aksesimit të platformës për përdoruesit e sistemeve Android ku kjo përqindje varion 25-30%. Paralelisht u projektua zgjidhja teknike e cila rrit efikasitetin pavarësisht llojit të platformës së përdorur nga përdoruesi, e quajtur Deep Packet Inspection (DPI). Me implementimin e kësaj zgjidhje teknike tek ofruesit e shërbimit të internetit mobile dhe fiks, efiçensa e bllokimit të platformës TikTok është e plotë.

Çfarë është Deep Packet Inspection (DPI)?

DPI është një platformë e cila analizon në mënyrë të detajuar paketën e trafikut të internetit dhe identifikon se nga cilat shërbime/platforma gjenerohet ky trafik dhe në varësi të kushteve të vendosura paraprakisht, lejon ose e bllokon atë.

Çdo përmbajtje që transmetohet përmes internetit, për shembull, një bisedë në WhatsApp apo aplikime të ngjashme, një video në TikTok, apo një email, është si një **paketë** që transmetohet në mënyrë të enkriptuar përmes internetit.

Çdo shërbim në internet që i ofrohet përdoruesëve segmentohet në paketa, ku çdo paketë (payload) i shtohet një kokë (header) e cila do të shërbejë për të rrugëzuar trafikun, si edhe një bisht (Tail) për të garantur integritetin e saj. Payload-i që përmban informacionin është ajo që enkriptohet.

Adresa: Rruga “Papa Gjon Pali II” nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

Në rastin kur trafiku kalon përmes tuneleve të enkriptuar (Virtual Private Network) enkriptohet e gjitha dhe për të bërë rrugëzimin e paketës drejt destinacionit i shtohet një kokë (header) tjeter.

Platforma DPI analizon VETËM kokën (headerin) e paketës së protokollit të internetit IP dhe e ka teknikisht të pamundur të deshifrojë/ç`kodojë dhe analizojë vetë përmbajtjen e paketës (payload-in).

Komunikimet me përmbajtje që transmetohen në internet në vendin tonë, janë 100% të **enkriptuara** me çelsa të bazuar në algoritma asimetrik për shkëmbimin e tyre, si edhe simetrik për kodimin e përmbajtjes. Në këto kushte **DPI NUK** arrin të aksesojë dhe as të lexojë përmbajtjen e komunikimit.

DPI sheh vetëm që "diçka po dërgohet diku", **por nuk mund të identifikojë dërguesin, marrësin dhe as përmbajtjen e informacionit**.

Çfarë mund të Analizojë DPI?

- Mund të kuptojë cilën aplikacion po përdor, bazuar në analizën e signaturës, por pa e identifikuar se cili është ai/ajo që po e përdor (p.sh., TikTok, etj).
- Mund të kuptojë sa shpesh po përdoret një aplikacion i caktuar, bazuar në analizën e sjelljes dhe të formës ("traffic shape"), por sërish nuk mund të identifikoj se cili është ai/ajo që po e përdor.
- Mund të kuptojë pikun kohor kur përdoret më shpesh një aplikacion, bazuar në analizën e "*timestamp*" e vendosur në kokën e paketës, por pa e identifikuar se cili është ai/ajo që po e përdor.
- Mund të **bllokojë** disa lloje trafiku, për shembull një platformë të caktuar, sulmet volumetrike (DDoS), sulmet kërcënuese (malware, ransomware), fushatat phishing, etj.

Si është e implementuar teknika DPI në vendin tonë ?

Implementimi i teknikës DPI në Shqipëri është i ndarë në dy faza:

1- Faza e parë mbulon kompanitë celulare Vodafone dhe One.
2- Faza e dytë mbulon të gjithë ofruesit e shërbimit të internetit me shumicë (Wholesale), të cilët shërbejnë si ndërmjetës midis pikave të hyrjes së internetit në vendin tonë dhe ofruesve të tjerë të shërbimit të internetit.

Për ngritjen e kësaj platforme AKSK ka punuar ngushtësisht me Autoritetin e Komunikimeve Elektronike dhe Postare, Komisionerin për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, si edhe me të gjithë ofruesit e shërbimit të internetit me shumicë (Wholesale ISP).

AKSK ka sqaruar ofruesit e shërbimit të internetit lidhur me disa çështje të ngritura prej tyre.

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

A mund të ndodhë përgjimi i komunikimeve nga përdorimi i platformës DPI?

Jo, nuk mund të ndodhë, pasi platforma DPI është vendosur në portën hyrëse të ofruesve të internetit.

Disa prej shërbimeve më të shpeshta që transmetohen nga ofruesit e internetit janë:

I. Faqet Web – Trafiku i të cilave është i enkriptuar dhe përdor protokollet *HTTPS over SSL/TLS.*

II. Email-i – Trafiku i të cilës është i enkriptuar dhe përdor protokollet SMTPS, IMAPS dhe POP3S.

III. Mediat Sociale – Platformat e komunikimit në masë si WhatsApp, Signal, Viber, Facebook, Instagram etj: Përdorin ekriptimin *end-to-end*, ç`ka do të thotë se trafiku është plotësisht i enkriptuar/koduar, i **PA AKSESUESHËM** dhe i **PA LEXUESHËM** midis dërguesit dhe marrësit.

IV. Akses në distancë (*Remote Access*) – Trafiku i të cilës është i enkriptuar dhe përdor protokollin SSH për kapje në distancë (Shërbimet e pasigurta Telnet/RDP nuk përdoren më në kohët e sotme, ose shfrytëzohen për qëllime të brendshme testimi prej specialistëve të IT-së).

V. Transferim skedarësh – Trafiku i të cilës është i enkriptuar dhe përdor protokollin SFTP (Protokolli i pasigurtë FTP/21 është prej kohësh i braktisur dhe nuk rekomandohet).

VI. Transferim të log-eve – Trafiku i të cilës është i enkriptuar dhe përdor protokollin SNMPv3 priv/auth. Përgjithsisht ky shërbim nuk kalon përmes internetit por përdoret gjerësisht në rrjetet LAN/Intranet. (Protokolli i pasigurtë SNMP v1/2 përdoret vetëm për qëllime të brendshme testimi prej specialistëve të IT-së).

Platforma DPI e ngritur në ofruesit e shërbimit të internetit në vendin tonë, analizon VETËM kokën (headerin) e paketës së protokollit IP dhe NUK KA ASNJË MUNDËSI TEKNIKE të deshifrojë/ç`kodojë dhe analizojë vetë paketën (payload), për shkak se ajo është e enkriptuar me çelsa asimetrik të gjatë për shkëmbimin e tyre dhe çelsa simetrik të avancuar për ruajtjen e përmbajtjes.

Të dhënat që analizohen nga DPI e instaluar tek ofruesit e shërbimit të internetit në vendin tonë janë:

- IP Publike burim/destinacion.
- Tipi i protokollit të përdorur.
- Numrin e portës së përdorur.
- Madhësinë dhe frekuencën e paketës së përdorur (*Traffic shape*).

Adresa: Rruga “Papa Gjon Pali II” nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

- Nënshkrimin (signaturën) e protokollit për të identifikuar në rastin konkret Tik Tok.
- Kohën e dërgimit/marrjes së paketës (timestamp).

DPI e instaluar në ofruesit e shërbimit të internetit NUK akseson dhe NUK lexon informacion në lidhje me:

- Përmbajtjen e mesazheve text, video, zanore nga platforma të ndryshme sociale, VOIP, Video-on-demand, email, share folder, etj.
- Të dhënat e përdoruesve.
- Kredencialet e Autentifikimit.
- Identitetin e individit (dërguesit dhe marrësit fundorë).
- Metadatat (pasi janë te enkriptuara në platformat e sotme).

Përfundimisht, platforma DPI e instaluar tek ofruesit e shërbimit të internetit ***NUK KA AFTËSI TEKNIKE PËR TË REALIZUAR ÇFARËDOLLOJ PËRGJIMI TË TRAFIKUT TË INTERNETIT***.

A cënohen të dhënat personale të përdoruesve nga përdorimi i platformës DPI ?

Jo. Nisur nga sa më sipër, të gjitha informacionet e analizuara nga DPI, nuk përbëjnë informacion sensitiv, psh. IP-ja publike mund të gjendet lehtësisht me një kërkim të thjeshtë me anë të motorrëve të kërkimit google, shodan, etj. Ndërkohë, asnjë nga informacionet e përpunuara nga platforma DPI të instaluara pranë ofruesve të shërbimit të internetit, nuk identifikon individin, për arsye se :

a. Përdoruesit që përdorin protokollin e komunikimit IPv4 (98,7% e përdoruesve në vendin tonë), identifikohen përmes IP-ve private, e cila fshehet pas një teknike të quajtur NAT dhe që është e **pa aksesueshme** dhe e kontrollueshme nga platforma DPI.

b. Përdoruesit që përdorin protokollin e komunikimit IPv6 në nivel individësh (1,3%) janë të mbrojtur për shkak se platformat e sotme përdorin automatikisht *Privacy Extension Header IPv6* (Android, iOS, Windows, macOS, Linux).

Gjithashtu, informacionet që lidhen me protokollin e komunikimit, portat e komunikimit, madhësinë e paketës, frekuencën si edhe signaturën e paketës, nuk lidhen me të dhëna identifikuese të individit por me vetë aplikacionin ose/edhe shërbimin që përdoret.

Platforma DPI e instaluar në operatorët e ofrimit të shërbimit të internetit është në përputhje me standardet e sigurisë së informacionit dhe GDPR ***G**eneral **D**ata **P**rotection **R**egulation* .

Adresa: Rruga “Papa Gjon Pali II” nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

A cënohet konkurenca e lirë nga implementimi i platformës DPI në mënyrë jo diskriminuese dhe proporcionale, ndaj të gjithë ofruesve të shërbimit të internetit ?

Me qëllim garantimin e konkurencës së lirë, AKSK në bashkëpunim me AKEP ka marrë masat e mëposhtme:

a. Kërkesat për bllokimin e DNS/SNI/IP i dërgohen përmes AKEP, **TË GJITHË** ofruesve të shërbimit të internetit;
b. Kërkesat për bllokimin e CDN-ve që transportojnë paketa Tik Tok i dërgohet **TË GJITHË** ofruesve të mëdhenj ndërkombëtar të këtyre shërbimeve ;
c. Kërkesat për mos shfaqjen e Tik Tok për përdoruesit me kartë SIM shqiptare ose/edhe me vendndodhje në vendin tonë, për platformat AppStore dhe PlayStore janë globale dhe të aksesueshme për **TË GJITHË** përdoruesit ;
d. Instalimi i DPI u krye në të **DY** kompanitë celulare që operojnë në vend ;
e. Instalimi i DPI do të vijojë për të **9 (NËNTË)** kompanitë e ofrimit të shërbimit të internetit me shumicë (ISP Wholesale) që mbulojnë territorin e vendit.

A mund të cënohet integriteti i të dhënave përmes përdorimit të kësaj teknologjie të instaluar në kompanitë e ofrimit të shërbimit të internetit?

Jo, në asnjë mënyrë. DPI-ja e instaluar tek ofruesit e shërbimit të internetit nuk modifikon përmbajtjen e paketave të trafikut të internetit, nuk ri-drejton trafikun, si edhe nuk dekripton këtë trafik.

Si pjesë e zgjidhjes teknike, pranë AKEP është implementuar Qendra e Monitorimit, e cila lidhet nëpërmjet një Tuneli të sigurtë (të enkriptuar) VPN LAYER2 me platformën e instaluar pranë operatorëve.

Roli i Qendrës së Monitorimit është si më poshtë:

a. Ka rolin e Administratorit tek të gjithë platformat e instaluara DPI në kompanitë e Ofrimit të Shërbimit të Internetit si edhe në vetë AKEP.

   Përcakton dhe rifreskon rregullat në DPI për bllokimin e paketave me përmbajtje Tik Tok. Këto rregulla përgjithësisht përcaktohen herën e parë dhe vetëm në raste të veçanta mund të ndryshojnë, duke ruajtur gjithmonë transparencën me operatorët e shërbimeve të internetit.

b. Përdorimin e protokollit "snmp v3 auth-priv" për të dërguar mesazhe njoftimi të nivelit alert nga pajisja DPI e instaluar pranë operatorëve të shërbimit drejt Qendrës së Kontrollit, për rastet e monitorimit të hardwar-it:

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

1. Djegie e Hard Disk Drive
2. Bllokim i konfigurimit të Hardisqeve
3. Rritje e kapacitetit të trafikut
4. Rritje e ngarkesës së CPU-së (CPU Overloading)
5. Rritje e hapësirës në memorjen dinamike RAM
6. Probleme fizike të rrjetit (psh, këputje e kabëllit)
7. Ndërprerje e energjisë
8. Dështim i bllokut të ushqimit

c. Rifreskimi i signaturave të Tik Tok, i cili normalisht do të kryhet sipas rastit dhe nevojës sipas procedurës së mëposhtme:

Signaturat e rifreskuara të TIK TOK, pasi të testohen në ambjentin laboratorik të qendrës së monitorimit nga ekspertët e Autoritetit Rregullator, do të dërgohen në mënyrë automatike drejt pajisjeve DPI të instaluara pranë kompanive të ofrimit të internetit përmes lidhjes tunel të sigurtë VPN L2TP.

Theksojmë se, ambjenti laboratorik në Autoritetin Rregullator ku ngarkohen signaturat e reja të Tik Tok, është tërësisht i izoluar dhe nuk ka asnjë mundësi aksesimi me ambjentin prodhim *(production*), të lidhur drejtpërdrejtë me pajisjen DPI. Frekuenca e ngarkimit të signaturave do të jetë rast pas rasti, menjëherë pas nxjerrjes nga platforma Tik Tok të signaturave të reja.

Të gjithë shërbimet e menaxhimit dhe përditësimit të platfomave DPI si dhe qendrës së monitorimit do të kryhen dhe aksesohen brenda territorit të vendit tonë.

Bazuar në opinionin zyrtar të Komisionerit për të drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, Zyra e Komisionerit vlerëson se, duke u bazuar në informacionin e referuar nga AKSK në lidhje me instalimin e DPI-së pranë ofruesve të shërbimeve të internetit, ndërmarrja e hapave teknike nga ana e operatorëve dhe AKEP nuk bie ndesh me dispozitat e Ligjit nr. 124/2024, "Për Mbrojtjen e të dhënave Personale".

Ekspertiza

Bazuar në nenin 3, pika 8 të marrëveshjes së bashkëpunimit të datës 6 Shkurt 2023, midis Autoritetit Kombëtar të Sigurisë Kibernetike dhe Autoritetit të Sigurisë Kibernetike të Izraelit (National Cyber Directorate of the State of Israel), është dërguar kërkesë për mbështetje në ekspertizë teknike dhe logjistike për implementimin e teknikave sa më eficiente për bllokimin e platformës TikTok në Republikën e Shqipërisë nga partnerët tanë Izraelitë, të cilët kanë shprehur dakortësinë për të na mbështetur.

Për implementimin e teknikës DPI jemi mbështetur nga homologët tanë Izraelit, të cilët kanë ofruar suport logjistik dhe ekspertizë teknike.

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

Mbështetja logjistike konsiston në ofrimin e platformës dhe pajisjeve të nevojshme hardware/software të cilat i janë ofruar AKSK-së në huapërdorim (Jo donacion), pa kosto financiare, për një periudhë 12-mujore.

Implementimi teknik pranë operatorëve është kryer nga ekspertët e AKSK-së dhe ekspertët Izraelit.

A mund të profilizohet sjellja e individit si pasojë e një ndërhyrje në të dhënat e përpunuara nga platformat DPI të instaluara në ofruesit e shërbimit të internetit ?

Nga të dhënat e analizuara nga platforma DPI, nuk mund të krijohet profil i sjelljes në nivel individi për arsye se siç dihet, trafiku në internet rrugëzohet përmes protokollit IP i cili klasifikohet në dy klasa :

1- IPv4 – Rreth 98,7% (të dhëna të marra në mënyrë empirike nga ekspertët e ofruesve të shërbimit të internetit në vendin tonë) e trafikut në Shqipëri rrugëzohet përmes këtij protokolli. Rrugëzimi i paketave të shërbimeve në internet realizohet VETËM përmes të ashtuquajturave IP Publike, të cilat janë të vetmet të cilat mund të shërbejnë për të bërë rrugëzimin e trafikut në internet. Këto IP publike në mbi 95% të rasteve i përkasin entiteteve publike dhe private. Për këtë arsye informacioni i cili përpunohet nga DPI dhe që i përket vetëm kokës (headerit) të protokollit të internetit IP publik nuk ka të bëjë me individin por me vet entitetin.
2- IPv6 – Rreth 1,3% (të dhëna të marra në mënyrë empirike nga ekspertët e ofruesve të shërbimit të internetit në vendin tonë) e trafikut në Shqipëri rrugëzohet përmes këtij protokolli. Ky protokoll arrin të rrugëzojë trafik “end to end”. Pavarësisht kësaj, edhe në këtë rast të gjithë platformat e mëposhtme kanë të integruar teknikën e sigurisë (Enkriptim/Enkapsulim për nivelin data dhe authentikim) të ashtuquajtur IPSec i cili përfshin teknikat Authentication Header (AH) dhe Encapsulating Security Payload (ESP) për trafikun IPv6.

Platformat e mëposhtme e kanë tashmë të integruar në kokën (header-in) e protokollit IPv6 këtë teknikë, duke e bërë të pamundur zbulimin e identitetit dhe profilin e sjelljes së klientit fundor(individit). Më konkretisht:

- Që prej vitit 2008 Microsoft e ka të zgjidhur këtë problem në sistemet operative Windows Server dhe që prej vitit 2006 e ka zgjidhur këtë problem për përdoruesit fundor (Tek Windows Vista është instaluar për herë të parë).
- Që prej vitit 2020 e ka të zgjidhur këtë problem në sistemet Linux Ubuntu 20.04 LTS.
- Debian 10 – që prej vitit 2019 e ka të zgjidhur këtë problem.
- Red Hat Enterprise Linux 7 – që prej vitit 2014 e ka të zgjidhur këtë problem.
- Fedora 38 – që prej vitit 2023 e ka të zgjidhur këtë problem.
- SUSE 12 – që prej vitit 2011 e ka të zgjidhur këtë problem.

Adresa: Rruga “Papa Gjon Pali II” nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

- macOS 10.7 (Platforma e operimit e kompanisë Apple) – që prej vitit 2011 e ka të zgjidhur këtë problem.
- iOS 4 (Platforma e operimit në telefonat iPhone e kompanisë Apple) – që prej vitit 2010 e ka të zgjidhur këtë problem.
- Android 4.0 (Platforma e operimit në telefonat Samsung, Google Pixel, One Plus, Xiaomi, Motorola, Nokia, OPPO, VIVO, Sony, Blackberry, ZTE, ASUS, etj) – që prej vitit 2011 e kanë të zgjidhur këtë problem.

Përfundimisht, nisur nga më sipër, edhe nëse do të kërkohej të realizohej një profil i sjelljes në nivel individi (pra, ç`farë programi ka përdorur një përdorues, apo kohën kur është hapur ky program, etj), duke ndërhyrë në platformën DPI, do të ishte e pamundur teknikisht për t'u realizuar.

Për individët (më pak se 5% e tregut) të cilët zotërojnë IP publike, sugjerohet përdorimi i shërbimeve përmes teknikave të sigurta të enkriptimit, me qëllim garantimin e MOSPROFILIZIMIT të sjelljes së tyre gjatë lundrimit në internet.

Megjithatë theksojmë se, qëllimi i vetëm i përdorimit të platformës DPI është bllokimi i aksesit të platformës TikTok në territorin e Republikës së Shqipërisë dhe jo profilizimi i sjelljeve të individëve.

Janë marrë një sërë masash shtesë teknike për kufizimin e përdorimit të platformës për qëllime të tjera, përfshirë ndalimin e aksesit të operatorëve të shërbimit të internetit në platformën DPI.

A ka rrezik të mbetet informacion pas rikthimit të platformës tek partnerët?

Jo, pasi log-et e mbetura në pajisjet që mundësojnë pajisjen do të fshihen përmes teknikave të sigurta të enkriptimit simetrik ose do të asgjësohen (vetem disqet ku ruhet informacioni) fizikisht, duke ndjekur rigorozisht proçedurat e përshkruara në standardin ndërkombëtar të sigurisë së informacionit ISO 27001.

Pse nuk u implementua kjo teknologji tek Ofruesit e Sherbimeve te Internetit në Shqipëri, por u mor përsipër nga vetë shteti Shqiptar?

Janë dy arsye:

a. Nëse do t`i lihej në dorë kompanive të ofrimit të shërbimit të internetit instalimi i teknikës DPI, shumica prej tyre nuk do të kishin kapacitetet dhe ekspertizën e nevojshme për t`a implementuar atë. Kjo do të bënte që të ndodheshim para një asimetrie në treg.

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

b. Kompanitë që do të bënin investime në implementimin e teknikës DPI, do të kishin monopolin e tregut dhe kjo mund të shkaktonte një rritje të kostove të internetit për qytetarët.

A është e implementuar platforma DPI në vendet e Bashkimit Europian ?

Po, janë shumë vende të Bashkimit Europian që për qëllime të mbrojtjes së fëmijeve dhe qytetarëve, sigurisë kombëtare, etj. e kanë të integruar këtë teknologji. Disa prej shteteve janë si më poshtë :

a. Franca – E përdor për çështjet e sigurisë kombëtare.
b. Gjermania – E përdor për çështjet e sigurisë kibernetike ndaj infrastrukturave kritike të vendit.
c. Hollanda – E përdor për çështjet e sigurisë kibernetike ndaj infrastrukturave kritike të vendit.
d. Polonia – E përdor për çështjet e sigurisë kibernetike ndaj infrastrukturave kritike të vendit.
e. Belgjika – E përdor për çështjet e sigurise kombëtare.
f. Hungaria – E përdor për çështjet e sigurisë kibernetike ndaj infrastrukturave kritike të vendit.
g. Republika Çeke – E përdor për çështjet e sigurise kombëtare.
h. Italia – E përdor për çështjet e sigurisë kibernetike ndaj infrastrukturave kritike të vendit.
i. Suedia
j. Finlanda – E përdor për çështjet e sigurisë kibernetike ndaj infrastrukturave kritike të vendit.
k. Spanja – E përdor për çështjet e sigurisë kibernetike ndaj infrastrukturave kritike të vendit.

Cilat janë disa nga vendet e avancuara në mbarë botën në teknologji që përdorin teknikën DPI (Përveç atyre të përmendura nga Bashkimi Europian) ?

a. Shtetet e Bashkuara të Amerikës – Për menaxhimin dhe kontrollin e trafikut.
b. Britania e Madhe – Për Sigurinë Kombëtare.
c. Izraeli – Për mbrojtjen kibernetike të infrastrukturave kritike të vendit.
d. Singapori – Për menaxhimin dhe kontrollin e trafikut, etj…

Adresa: Rruga “Papa Gjon Pali II” nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

Konkluzione

1- Platforma DPI e ka të pamundur teknikisht dhe shkencërisht të bëjë përgjim të komunikimeve.
2- Platforma DPI e ka të pamundur teknikisht dhe shkencërisht të prekë të dhënat e individit, pasi të gjithë komunikimet që transmetohen në internet janë të enkriptuara/koduara (përjashtim bëjnë vetëm rastet studimore).
3- Platforma DPI e ka të pamundur teknikisht dhe shkencërisht të profilizojë sjelljen në nivel individi, pasi trafiku në internet në 98,7% të rasteve është me IPv4 Publike (Ku në 95% të rasteve është në nivel entiteti (jo individi)) dhe 1,3% të rasteve është me IPv6 e cila përdor kokë shtesë (extension header) të mbështetur në teknikën enkriptuar IPSec (ESP/AH). Rastet përjashtimore mund të rregullohen përmes disa kushteve të veçanta teknike, si:
   a. Përdorimi i tuneleve të sigurtë i trafikut të dhënave
   b. Rregullat Përjashtimore të përcaktuara qartë midis AKEP, AKSK, Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, si edhe vetë kompanive të Ofrimit të Shërbimit të Internetit.
4- Platforma DPI përdoret gjerësisht në vendet e Bashkimit Europian dhe vendet e tjera demokratike të botës për mbrojtjen e Sigurisë Kombëtare, Infrastrukturave kritike, Qytetareve, Menaxhimin dhe Kontrollin e Trafikut.
5- Platforma DPI identifikon dhe më pas bllokon vetëm paketat TikTok të cilat transmetohen në rrjet pa zbuluar përmbajtjen e tyre, sepse kjo realizohet përmes "signaturave" të kësaj platforme të lokalizuara në kokën e paketës së protokollit të rrugëzimit të internetit IP.
6- AKSK dhe AKEP kanë zbatuar parimin e konkurrencës së lirë, mosdiskriminimit dhe proporcionalitetit me transparencë të plotë. Çdo iniciativë për zgjidhje teknike është kryer njëkohësisht për të gjitha kompanitë e ofrimit të shërbimit të internetit (Wholesale) sipas marrëveshjeve kontraktuale me to. Ekzekutimi dhe vazhdimi i mëtejshëm i projektit do të kryhet në formë horizontale (pra, ekzekutimi për bllokimin e platformës TikTok për rrjetin fiks, në të gjitha kompanitë, do të kryhet në të njëjtën kohë).

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039