REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

METODOLOGJIA KOMBËTARE E VLERËSIMIT TË RREZIKUT TË SIGURISË KIBERNETIKE

Përmbajtja

1. Hyrje

Shqipëria, herë pas here është përballur me sulme kibernetike ndaj operatorëve që ofrojnë shërbime kritike dhe të rëndësishme. Përpjekjet e vazhdueshme në digjitalizimin e shërbimeve, sjellin lehtësime dhe fleksibilitet në funksionet jetësore, shoqërore dhe ekonomike të qytetarëve, por nga ana tjetër rrisin mundësinë e ndodhjes së sulmeve kibernetike duke vënë në pah ndërvarësinë dhe ndërlidhjen gjithnjë e më shumë të sistemeve të teknologjisë së informacionit mes tyre. Gjithashtu varësia nga zinxhirët globalë të furnizimit do të thotë që organizatat janë gjithashtu të ekspozuara ndaj rreziqeve sistemike kibernetike jashtë kontrollit të tyre të drejtpërdrejtë dhe si rrjedhim bëhen më të ndjeshme ndaj efekteve të menjëhershme ndërprerëse të sulmeve kibernetike.

Për të kuptuar, përmirësuar dhe për një vendimmarrje sa më të favorshme në kuadër të pozicionit të rrezikut kombëtar të sigurisë kibernetike, AKSK duhet të kuptojë vazhdimisht rreziqet e sigurisë kibernetike që lidhen me çdo sektor ku operojnë OIKI/OIRI-të dhe të bashkëveprojë në identifikimin e rreziqeve kibernetike. Krijimi i besimit dhe bashkëpunimi me operatorët është shumë i rëndësishëm për identifikimin dhe zbutjen e rreziqeve të sigurisë kibernetike.

Ky dokument prezanton Metodologjinë Kombëtare të Vlerësimit të Rrezikut të Sigurisë Kibernetike (*Në vijim Metodologjia)* për Hapësirën Digjitale Kombëtare. Autoriteti Kombëtar i Sigurisë Kibernetike (AKSK) zhvilloi këtë proces analitik të standardizuar nëpërmjet qasjes nga poshtë-lart (siç ilustrohet në Figurën 1), të kontekstualizuar me inteligjencën e kërcënimeve kibernetike dhe informacioneve të tjera. Metodologjia bazohet në standardet[1] dhe praktikat ndërkombëtare më të mira të menaxhimit të rrezikut kibernetik dhe është në përputhje me Kërkesat e Direktivës të Bashkimit Evropian (NIS2).

[1] ISO 27001/5, ENISA and NIST SP 800-53

Kjo metodologji konsiston në tre hapa kryesore:

- Hapi 1. Operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit (OIKI/OIRI) kryejnë vlerësime individuale të rrezikut të sigurisë kibernetike.
- Hapi 2. AKSK, kryen vlerësime sektoriale të rrezikut të sigurisë kibernetike.
- Hapi 3. AKSK, kryen vlerësimin kombëtar të rrezikut të sigurisë kibernetike.

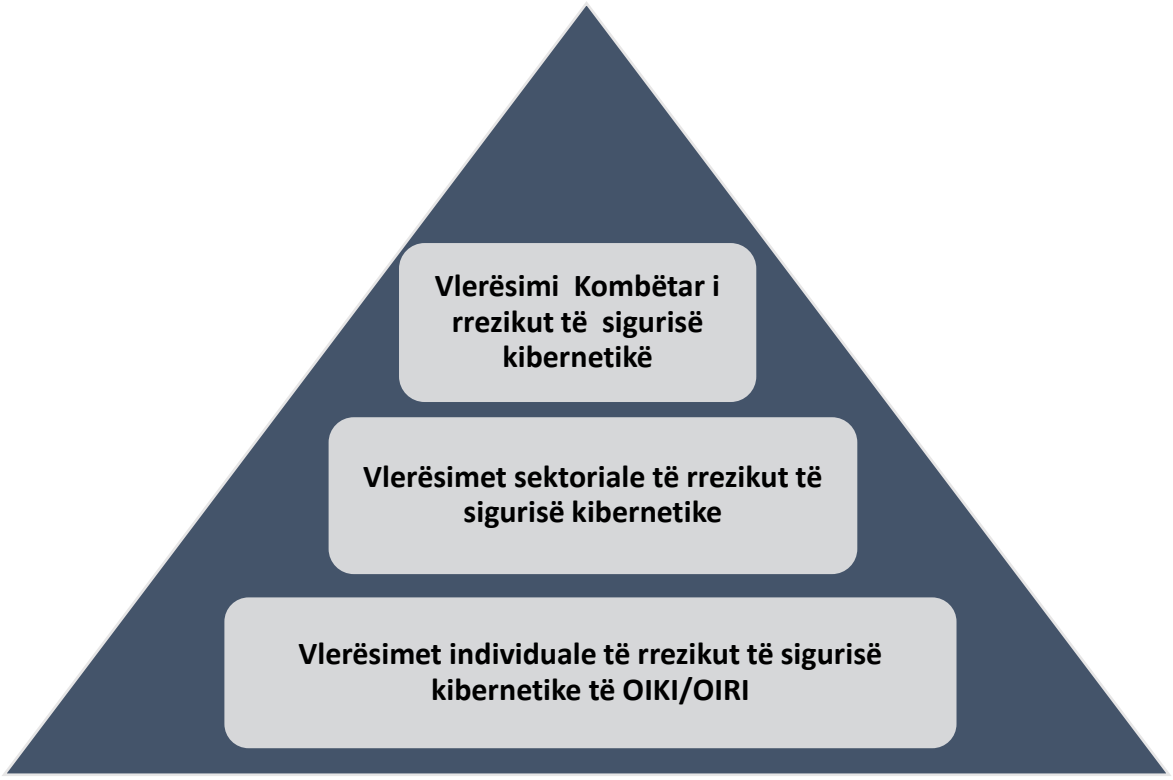

Figura 1 Tre nivelet e vlerësimit të rrezikut

2. Zbatueshmëria

Metodologjia Kombëtare e Vlerësimit të Rrezikut të Sigurisë Kibernetike është hartuar në zbatim të Ligjit Nr. 25/2024, *"Për sigurinë kibernetike",* për të krijuar një qasje të unifikuar, transparente në vlerësimin e rreziqeve kibernetike që kërcënojnë shërbimet e rëndësishme dhe kritike në Shqipëri.

Si pjesë e kësaj qasjeje, çdo OIKI/OIRI është:

- Përgjegjës për identifikimin dhe menaxhimin e rreziqeve të organizatës dhe shërbimet që ofrojnë, duke zbatuar praktikat më të mira të sigurisë kibernetike dhe kontrollet e aplikueshme në përputhje me standardet ndërkombëtare, për të mbrojtur dhe ruajtur konfidencialitetin, integritetin dhe disponueshmërinë "*CIA"* të shërbimeve dhe të dhënave të saj.
- Përgjegjës për realizimin e vlerësimit periodik të rrezikut kibernetik (të paktën një herë në vit), ose në rast ndryshimesh të klasifikuara si madhore nga vetë operatori.

OIKI/OIRI mund të zgjedhë sipas vendimmarrjes individuale metodologjinë e vlerësimit të rrezikut kibernetik bazuar në standardet ndërkombëtare, por duhet të raportojë pranë AKSK-së, mbi vlerësimin e rrezikut sipas specifikimeve në këtë metodologji (sipas template të përcaktuar nga AKSK).
AKSK do të përdorë këtë metodologji për të vlerësuar rrezikun kibernetik nga niveli i infrastrukturës, sektorial e deri në atë kombëtar.

3. Qëllimi

Metodologjia Kombëtare e Vlerësimit të Rrezikut Kibernetik synon të sigurojë një kornizë gjithëpërfshirëse për identifikimin, vlerësimin, zbutjen dhe menaxhimin e rreziqeve kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit. Metodologjia siguron identifikimin e dobësive, vlerësimin e ndikimeve të mundshme dhe zbatimin e strategjive efektive të menaxhimit të rrezikut. Ajo përfshin një gamë faktorësh, përfshirë analizën e kërcënimeve, vlerësimin e rëndësisë së aseteve dhe planifikimin e qëndrueshmërisë, duke mundësuar që operatoret të përmirësojnë qëndrueshmërinë kibernetike dhe të kontribuojnë në mbrojtjen e sigurisë kombëtare, stabilitetin ekonomik dhe sigurinë publike.

4. Objektivat

Objektivat e Metodologjisë Kombëtare të Vlerësimit të Rrezikut Kibernetik adresojnë dhe menaxhojnë në mënyrë sistematike rreziqet kibernetike në infrastrukturën kombëtare dhe ekosistemet dixhitale.

Objektivat kryesore përfshijnë:

- Identifikimin dhe vlerësimin e kërcënimeve dhe dobësive kibernetike për infrastrukturat e rëndësishme dhe kritike të informacionit.
- Prioritizimin e rreziqeve bazuar në ndikimin e tyre të mundshëm për të siguruar shpërndarjen efektive të burimeve.
- Zhvillimin e strategjive me qëllim zbutjen e rreziqeve për të përmirësuar sigurinë kibernetike kombëtare.
- Promovimin e bashkëpunimit midis palëve të interesuara për të nxitur një qasje të unifikuar ndaj sigurisë kibernetike.
- Përmirësimin e aftësive për përgjigje ndaj incidenteve për të adresuar shpejt dhe në mënyrë efektive incidentet kibernetike.
- Sigurimin e qëndrueshmërisë dhe vazhdimësisë së shërbimeve kritike përballë kërcënimeve kibernetike në zhvillim.

5. Fusha e Veprimit

Metodologjia fokusohet në identifikimin e rreziqeve të sigurisë kibernetike ndaj shërbimeve kritike dhe të rëndësishme të vendit, që lidhen me analizimin e faktorëve si: Njerëzit, Proceset, Teknologjia, Gjeopolitika (Çështje që lidhen drejtpërdrejtë me politikën kombëtare të vendit) dhe të tjera (Elementë të tjerë që nuk kanë lidhje me faktorët e mësipërm).

AKSK bazuar në këtë metodologji mbështet në këto objektiva specifike:

a. Vlerësimin e rrezikut të shërbimeve të operatorit të OIKI/OIRI me periodicitet 6 mujorë
b. Ri-vlerësimin e nivelit të rrezikut kibernetik të OIKI/OIRI pas një ndryshimi madhor (sipas përcaktimeve në ligjin e sigurisë kibernetike) në:
    - Arkitekturën e Sistemeve.
    - Shërbimeve të reja të ofruara.
    - Infrastrukturë.
    - Furnizimi i palëve të treta.
    - Bazën rregullative.
    - Strukturimin e ri të institucionit.
    - Rastin e një incidenti me impakt madhor, etj.

6. Burimet e informacionit për vlerësimin e Rrezikut Kibernetik

Për të vlerësuar rrezikun kombëtar lidhur me sigurinë kibernetike të vendit, AKSK analizon informacionet e marra nga:

- OIKI/OIRI përmes pyetësorëve me periodicitet 6-mujor (*Aneksi nr.1*),
- Raportet e Vlerësimit të Rrezikut Kibernetik të operatorëve,
- Raportet e Organit të Vlerësimit të Konformitetit,
- Raportet e auditimit të brendshme/jashtme nga OIKI/OIRI, apo të realizuara nga AKSK,
- Raportet dhe analiza te kryera nga AKSK ose OIKI/OIRI lidhur me Incidentet, Kërcënimet, TTP-të, Dobësitë, etj,
- Informacion nga Shërbimi e Inteligjencës, e Sigurisë dhe mbrojtjes,
- Informacion nga partnerët ndërkombëtarë,
- Media (sociale, portale, TV, e shkruar).

7. Regjistri i Rreziqeve i Operatorëve të Infrastrukturave Kritike dhe të Rëndësishme

Regjistri do të përbëhet nga profilet e operatorëve që do të përfshijë informacione bazë mbi infrastrukturat, arkitekturat e tyre, sistemet, shërbimet, zinxhirët e furnizimit të tyre si dhe informacione mbi vlerësimet e brendshme të rrezikut kibernetik bazuar në të dhënat e gjeneruara nga auditimet dhe testimet e realizuara. Në ndërtimin dhe popullimin e të dhënave të profilit të operatoreve, informacioni do të mblidhet nga të dhënat e disponueshme publike sikurse dhe nëpërmjet pyetësorëve *(Aneksi Nr. 1)* të detyrueshëm, të iniciuar dhe dërguar çdo operatori nga AKSK.

Informacioni i përdorur në metodologjinë e AKSK-së, do të ruhet në një bazë të dhënash të quajtur *Regjistri i Rreziqeve OIKI/OIRI*. AKSK do të mirëmbajë dhe përditësojë këtë regjistër nëpërmjet menaxhimit të duhur të “aksesit” dhe kontrolleve bazuar mbi principin "kërkesë sipas nevojës".

8. Hapat e implementimit të metodologjisë

Për implementimin e metodologjisë për vlerësimin e riskut në nivel kombëtar, AKSK do të ndjek hapat e mëposhtëm:

8.1 Mbledhja e informacionit

AKSK, kryen procesin e mbledhjes së informacionit bazuar në burimet e përcaktuara në pikën 7 të kësaj metodologjie.

8.2 Analiza dhe Vlerësimi i Riskut

- Analiza e informacioneve të mbledhura nga AKSK për identifikimin e rreziqeve,
- Vlerësimi i Rrezikut në formatet sasiore dhe cilësore për çdo OIKI/OIRI *(Aneksi Nr. 4),*
- Përfshirja e rreziqeve Gjeopolitike dhe Të tjera në vlerësimin e rrezikut kombëtar,
- Prioritizimi i rreziqeve,
- Vlerësimi i rreziqeve në nivel sektorial dhe kombëtar

8.3 Raportimi dhe Monitorimi.

AKSK, harton 2 herë në vit Raportin e Vlerësimit të Rrezikut Kombëtar.

Raporti i Vlerësimit të Rrezikut të Operatorit, do t`i dërgohet secilit prej OIKI/OIRI.

AKSK në mënyrë të vazhdueshme monitoron dhe vlerëson rrezikun kibernetik për trajtimin e tyre nga OIKI/OIRI sipas prioritizimit kohor të përcaktuar në Tabelën nr.9.