VENDIM
Nr. 308, datë 4.6.2025

PËR MIRATIMIN E METODOLOGJISË PËR VLERËSIMIN DHE ANALIZIMIN E RREZIKUT TË SIGURISË KIBERNETIKE

Në mbështetje të nenit 100 të Kushtetutës dhe të shkronjës "ë", të nenit 9, të ligjit nr. 25/2024, "Për sigurinë kibernetike", me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e metodologjisë për vlerësimin dhe analizimin e rrezikut të sigurisë kibernetike, sipas tekstit që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.
2. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike dhe operatorët e infrastrukturave kritike e të rëndësishme të informacionit për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

ZËVENDËSKRYEMINISTËR
Belinda Balluku

METODOLOGJIA PËR VLERËSIMIN DHE ANALIZIMIN E RREZIKUT TË SIGURISË KIBERNETIKE

Lista e figurave

Lista e tabelave

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 operatorët e infrastrukturave të informacionit janë, gjithashtu, të ekspozuar 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 e për një vendimmarrje sa më të favorshme në kuadër të pozicionit të rrezikut kombëtar të sigurisë kibernetike, Autoriteti Kombëtar për Sigurinë Kibernetike duhet të kuptojë vazhdimisht rreziqet e sigurisë kibernetike që lidhen me çdo sektor, ku operojnë OIKI-të/OIRI-të dhe të bashkëveprojë për 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 për vlerësimin dhe analizimin e rrezikut të sigurisë kibernetike" (në vijim "Metodologjia") për hapësirën digjitale kombëtare. Autoriteti Kombëtar për Sigurinë 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 përcaktimet e ligjit nr. 25/2024, "Për sigurinë kibernetike", dhe kërkesat e direktivës së Bashkimit Evropian (NIS2).

Kjo metodologji konsiston në tre hapa kryesorë:

- Hapi 1. AKSK-ja kryen vlerësime individuale të rrezikut të sigurisë kibernetike për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit (OIKI/OIRI), bazuar në burimet e përcaktuara në pikën 6 të kësaj metodologjie;
- Hapi 2. AKSK-ja kryen vlerësime sektoriale të rrezikut të sigurisë kibernetike;
- Hapi 3. AKSK-ja kryen vlerësimin kombëtar të rrezikut të sigurisë kibernetike.

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

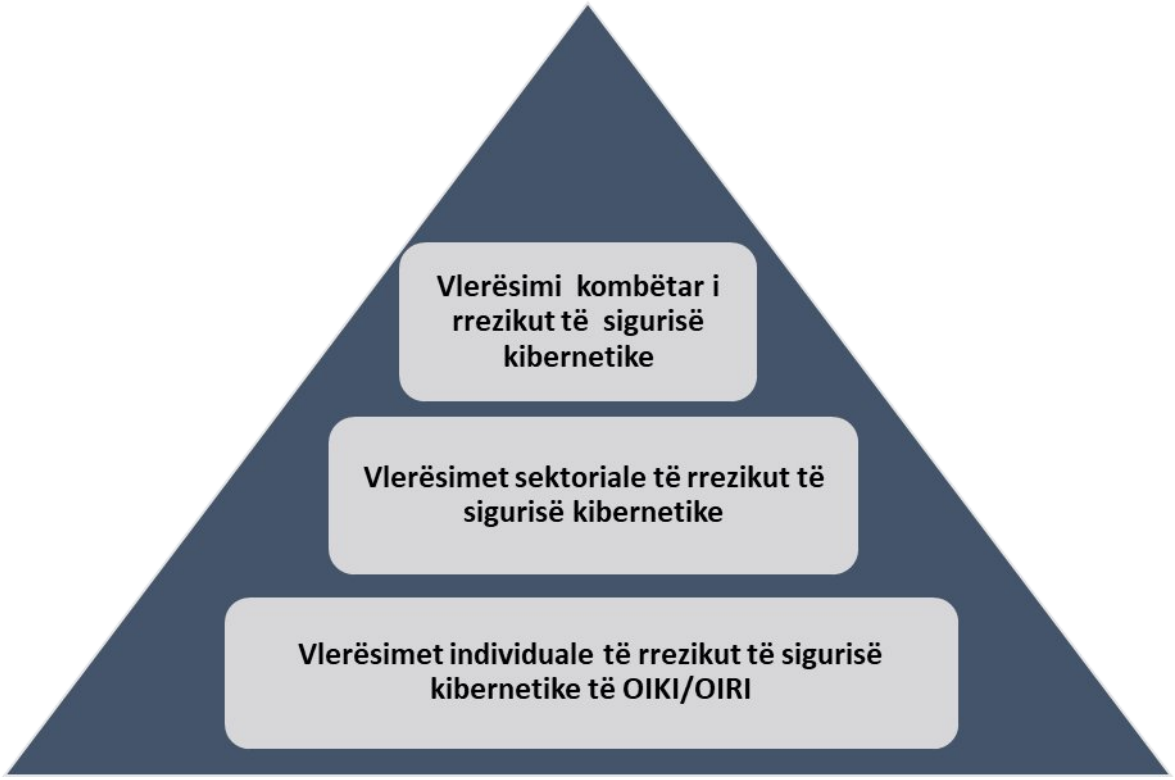

Figura 1. Tri nivelet e vlerësimit të rrezikut

2. Objekti

Objekti i kësaj metodologjie është vendosja e një kornize gjithëpërfshirëse për identifikimin, vlerësimin, zbutjen dhe menaxhimin e rreziqeve kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit, duke mundësuar që operatorët e infrastrukturave të përmirësojnë qëndrueshmërinë kibernetike dhe të kontribuojnë në mbrojtjen e sigurisë kombëtare, stabilitetin ekonomik dhe sigurinë publike.

3. Qëllimi

Qëllimi i kësaj metodologjie është identifikimi, analizimi dhe vlerësimi i dobësive në infrastrukturat e informacionit, me qëllim mbrojtjen e tyre, duke përmirësuar dobësitë në këto infrastruktura dhe duke garantuar qëndrueshmërinë kibernetike për të rritur nivelin e sigurisë kibernetike në nivel kombëtar.

4. **Përkufizimet**

Termat e përdorur në këtë metodologji kanë të njëjtin kuptim me termat e përcaktuar në ligjin nr. 25/2024, "Për sigurinë kibernetike".

5. Përgjegjësia e AKSK-së dhe OIKI-së/OIRI-së

AKSK-ja është përgjegjëse për vlerësimin e rrezikut kibernetik nga niveli i infrastrukturës, sektorial e deri në atë kombëtar, sipas përcaktimeve të kësaj metodologjie.

Çdo OIKI/OIRI është përgjegjës në lidhje me:

- identifikimin dhe menaxhimin e rreziqeve të infrastrukturës së informacionit dhe shërbimeve që ofrojnë, duke zbatuar praktikat më të mira të sigurisë kibernetike dhe kontrollet e aplikueshme, në përputhje me standardet ndërkombëtare, për të mbrojtur dhe për të ruajtur konfidencialitetin, integritetin dhe disponueshmërinë "CIA" të shërbimeve dhe të dhënave të saj;
- 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 sa herë i kërkohet nga AKSK-ja mbi vlerësimin e rrezikut, sipas specifikimeve në këtë metodologji (sipas formatit të përcaktuar nga AKSK-ja).

6. Objektivat

Objektivat kryesorë të kësaj metodologjie përfshijnë:

a) identifikimin dhe vlerësimin e kërcënimeve dhe dobësive kibernetike për infrastrukturat e rëndësishme dhe kritike të informacionit;

b) prioritizimin e rreziqeve bazuar në ndikimin e tyre të mundshëm për të siguruar shpërndarjen efektive të burimeve;

c) zhvillimin e strategjive me qëllim zbutjen e rreziqeve për të përmirësuar sigurinë kibernetike kombëtare;

ç) promovimin e bashkëpunimit ndërmjet palëve të interesuara për të nxitur një qasje të unifikuar ndaj sigurisë kibernetike;

d) përmirësimin e aftësive për përgjigje ndaj incidenteve për të adresuar shpejt dhe në mënyrë efektive incidentet kibernetike;

dh) sigurimin e qëndrueshmërisë dhe vazhdimësisë së shërbimeve kritike përballë kërcënimeve kibernetike në zhvillim.

6.1. Objektivat specifikë

AKSK-ja, bazuar në këtë metodologji, mbështetet në këta objektiva specifikë:

a) Vlerësimin e rrezikut të shërbimeve të OIKI-së/OIRI-së me periodicitet 6-mujor.

b) Rivlerësimin e nivelit të rrezikut kibernetik të OIKI-së/OIRI-së pas një ndryshimi madhor në:

- arkitekturën e sistemeve;
- shërbimet e reja të ofruara;
- infrastrukturën;
- furnizimin e palëve të treta;
- kuadrin rregullativ;
- ristrukturimin e institucionit;
- rastin e një incidenti me ndikim të lartë etj.

7. Fusha e veprimit

Metodologjia fokusohet në identifikimin e rreziqeve të sigurisë kibernetike ndaj shërbimeve të infrastrukturave kritike dhe të rëndësishme të informacionit të vendit, që lidhen me analizimin e faktorëve, si: burimet njerëzore, proceset, teknologjia, gjeopolitika (çështje që lidhen drejtpërdrejt me politikën kombëtare të vendit) dhe të tjera (elemente të tjera të rëndësishme që nuk janë të përfshirë në kategoritë e mësipërme, por që mund të ndikojnë në sigurinë kibernetike dhe që AKSK-ja i merr në konsideratë në varësi të zhvillimeve të reja teknologjike, ligjore, gjeopolitike ose operacionale).

8. Burimet e informacionit për vlerësimin e rrezikut kibernetik

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

- OIKI/OIRI përmes pyetësorëve me periodicitet 6-mujor, të cilët miratohen me urdhër të drejtorit të përgjithshëm të AKSK-së;
- raportet e vlerësimit të rrezikut kibernetik të operatorëve;
- raportet e organit të vlerësimit të konformitetit për sigurinë kibernetike;
- raportet e auditimit të brendshëm/jashtëm nga OIKI/OIRI apo kontrollit, të realizuara nga AKSK-ja pranë këtyre infrastrukturave të informacionit;
- raportet dhe analiza e kryer nga AKSK-ja ose OIKI/OIRI lidhur me incidentet, kërcënimet, teknikat e taktikat dhe procedurat që përdoren nga sulmuesi, dobësitë etj.;
- shërbimet e inteligjencës, të sigurisë dhe mbrojtjes;
- partnerët ndërkombëtarë;
- media (sociale, portale, TV, e shkruar).

9. Regjistri i rreziqeve të OIKI-t/OIRI-t

AKSK-ja do të ndërtojë, mirëmbajë dhe përditësojë një regjistër të rreziqeve OIKI/OIRI. Regjistri do të përbëhet nga profilet e operatorëve, që do të përfshijnë 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 kontrollet, auditimet, testimet e realizuara, raportet dhe analizat e kryera nga AKSK-ja ose OIKI/OIRI lidhur me incidentet, kërcënimet kibernetike. Në ndërtimin dhe popullimin e të dhënave të profilit të operatorëve, informacioni do të mblidhet nga të dhënat e disponueshme publike, sikurse dhe nëpërmjet pyetësorëve të detyrueshëm, të iniciuar dhe dërguar çdo operatori nga AKSK-ja.

AKSK-ja do të mirëmbajë e do të përditësojë këtë regjistër nëpërmjet menaxhimit të duhur të "aksesit" dhe kontrolleve bazuar në parimin "kërkesë sipas nevojës".

10. Hapat e implementimit të metodologjisë

Për implementimin e metodologjisë për vlerësimin dhe analizimin e rrezikut të sigurisë kibernetike në nivel kombëtar, AKSK-ja do të ndjekë hapat e mëposhtëm:

10.1. Mbledhja e informacionit

AKSK-ja kryen procesin e mbledhjes së informacionit bazuar në burimet e përcaktuara në pikën 8 të kësaj metodologjie.

10.2. Analiza dhe vlerësimi i rrezikut

Kjo fazë përfshin hapat e mëposhtëm:

a) analizën e informacioneve të mbledhura nga AKSK-ja për identifikimin e rreziqeve;

b) vlerësimin e rrezikut në formatet sasiore dhe cilësore për çdo OIKI/OIRI, sipas pikës 12 të kësaj metodologjie;

c) përfshirjen e rreziqeve gjeopolitike dhe të tjera në vlerësimin e rrezikut kombëtar;

ç) prioritizimin e rreziqeve;

d) vlerësimin e rreziqeve në nivel sektorial dhe kombëtar.

10.3. Raportimi dhe monitorimi

AKSK-ja harton 2 herë në vit raportin e vlerësimit dhe analizimit të rrezikut kombëtar, raport i cili do t'u dërgohet operatorëve të infrastrukturave të informacionit.

AKSK-ja, në mënyrë të vazhdueshme, monitoron e vlerëson rrezikun kibernetik, me qëllim trajtimin e rreziqeve nga OIKI/OIRI, sipas prioritizimit kohor të përcaktuar në tabelën nr. 6 të kësaj metodologjie.

11. Caktimi i peshave të pyetësorit

11.1. Detajimi i peshave (ndikimi) teknologjike

Sipas ndikimit teknologjik, peshat reflektojnë rëndësinë dhe ndikimin që ka secila masë teknike e sigurisë në "Pyetësor" në sigurinë e përgjithshme të sistemit, sipas ndikimit që mund të kenë në triadën e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave.

11.2. Detajimi i peshave (ndikimi) të proceseve

Sipas hendekut të proceseve, ndikimi do të jetë një shumatore e 5 (pesë) kategorive të marra në konsideratë nga standardi ISO 27005, si në vijim:

1. Ndikimi financiar

a) Humbjet e të ardhurave: Sulmet kibernetike mund të çojnë në humbje të ardhurash, për shkak të ndërprerjes së operacioneve ose ndërprerjes së shërbimeve;

b) Kostot e rikuperimit: Kostot e lidhura me zbulimin, përgjigjen dhe rikuperimin nga sulmet kibernetike mund të jenë shumë të larta;

c) Dëmet për shkak të mashtrimeve: Përfshirja në aktivitete të paligjshme, si vjedhja e identitetit ose mashtrimet financiare, mund të shkaktojë dëme të mëdha financiare.

2. Ndikimi ligjor dhe reputacional

a) Sanksionet dhe gjobat: Shkeljet e ligjeve dhe rregulloreve të privatësisë dhe sigurisë së të dhënave mund të rezultojnë në sanksione të rënda dhe gjoba;

b) Ndjekja penale: Operatorët e infrastrukturave mund të përballen me ndjekje penale dhe përgjegjësi ligjore për mosmbrojtjen adekuate të të dhënave të përdoruesve;

c) Humbja e besimit të klientëve: Incidentet e sigurisë mund të dëmtojnë besimin e klientëve dhe partnerëve, duke shkaktuar humbje të klientëve dhe të ardhurave të mundshme;

ç) Dëmtimi i markës: Një sulm kibernetik mund të dëmtojë imazhin dhe reputacionin e një operatori të infrastrukturës së informacionit, gjë që mund të ketë pasoja afatgjata në treg.

3. Ndikimi social

a) Shkeljet e privatësisë: Rreziqet kibernetike mund të shkaktojnë shkelje të privatësisë dhe të të dhënave personale të individëve, duke çuar në pasoja të rënda për jetën private;

b) Ndikimi në shëndetin dhe sigurinë e qytetarëve: Sulmet ndaj sistemeve shëndetësore dhe të sigurisë publike mund të kenë pasoja të rënda për shëndetin dhe sigurinë e qytetarëve.

4. Ndikimi operacional

a) Ndërprerja e shërbimeve: Sulmet *DDoS* (*Distributed Denial of Service)* dhe *malware* mund të ndërpresin shërbimet kritike, duke penguar funksionimin normal të operatorit të infrastrukturës dhe sistemeve.

b) Humbja e të dhënave: Të dhënat mund të fshihen, të shkatërrohen ose të vidhen gjatë sulmeve kibernetike, duke penguar operacionet dhe duke shkaktuar humbje të dhënash të rëndësishme.

5. Ndikimi në sigurinë kombëtare

a) Kompromentimi i infrastrukturës kritike të informacionit: Sulmet kibernetike ndaj infrastrukturës kritike të informacionit, si: energjia, uji, dhe shërbimet financiare etj. mund të kërcënojnë sigurinë kombëtare dhe jetën e qytetarëve;

b) Rreziku për mbrojtjen kombëtare: Sulmet ndaj sistemeve qeveritare dhe ushtarake mund të kërcënojnë sigurinë kombëtare dhe të ndikojnë në marrëdhëniet ndërkombëtare. Secili prej ndikimeve të mësipërme e ka peshën 0 ose 1. Shuma e peshave përcakton peshën totale të masës organizative të sigurisë.

11.3. Detajimi i peshave (ndikimi) të burimeve njerëzore

Peshat reflektojnë rëndësinë dhe ndikimin që ka secila masë teknike e sigurisë në sigurinë e përgjithshme të sistemit, sipas ndikimit që mund të kenë në hendekun e burimeve njerëzore (institucioni ka mjaftueshëm kapacitete të burimeve njerëzore për sigurinë kibernetike për të përmbushur qëllimet/objektivat strategjikë/operacionalë), si dhe hendekun profesional (kapacitete njerëzore me eksperiencën dhe kualifikimet e mjaftueshme për të përmbushur qëllimet/objektivat strategjikë/operacionalë).

Hendeku i burimeve njerëzore identifikon dhe vlerëson diferencën ndërmjet kapacitetit aktual të burimeve njerëzore dhe kërkesave optimale të nevojshme. Formula për vlerësimin e këtij hendeku mbështetet në praktikat më të mira të vlerësimit të kapaciteteve teknike dhe organizative në fushën e sigurisë kibernetike, duke u bazuar në parametrat kryesorë të përcaktuar në standardet ISO/IEC 27001 dhe 27005 për burimet njerëzore. Ky vlerësim bazohet në katër parametra kryesorë:

a) numrin total të punonjësve;

b) vendndodhjet gjeografike;

c) shërbimet kritike;

ç) numrin aktual të ekspertëve.

Formula e përdorur në këtë analizë është:

Hendeku i burimeve njerëzore = {(Numri total i punonjësve × 0.02[2]) + (Vendndodhjet gjeografike ÷ 30[3]) + (Shërbimet kritike ÷ 4[4])} – Numrin aktual të ekspertëve IT+Sec.

Hendeku profesional vlerësohet në bazë të peshës që sjell niveli i ekspertizës së punonjësit në fushën e sigurisë kibernetike. Kjo peshë përcaktohet duke marrë parasysh vitet e përvojës profesionale, zotërimin e certifikimeve të njohura ndërkombëtarisht, si dhe të diplomave apo të certifikimeve të lëshuara nga institucione të arsimit profesional dhe të lartë të akredituara në Republikën e Shqipërisë, në fusha të tilla, si: teknologjia e informacionit, siguria kibernetike, inxhinieria, apo shkencat kompjuterike.

---

[2] Shumëzimi i numrit total të punonjësve me 0.02 pasqyron një pjesë të vogël, por të rëndësishme të forcës së punës që kërkohet për të mbajtur operacionet optimale.

3 Ndarja e numrit të vendndodhjeve gjeografike me 30 normalizon të dhënat, duke i bërë ato të krahasueshme me parametrat e tjerë.

4 Ndarja e shërbimeve kritike me 4 llogarit rëndësinë e këtyre shërbimeve në efikasitetin e përgjithshëm operacional.

Tabela në vijim prezanton peshën në këndvështrim të hendekut profesional:

Tabela nr. 1 Pesha sipas hendekut profesional

Vitet e eksperiencës në fushën e sigurisë kibernetike	Certifikime ndërkombëtare në fushën e sigurisë kibernetike	Pesha
3	0	1
2	1	1
1	2	1
2	0	2
1	1	2
1	0	3
0	1	4
0	0	5

12. Vlerësimi i rrezikut

Në këtë fazë shpjegohet procesi i vlerësimit dhe i analizimit të rrezikut të sigurisë kibernetike të përdorur në këtë metodologji, duke përfshirë identifikimin, vlerësimin dhe trajtimin e rrezikut kibernetik kombëtar, që mund të cenojë infrastrukturat kritike dhe të rëndësishme të informacionit të vendit.

Metodologjia e vlerësimit dhe e analizimit të rrezikut të sigurisë kibernetike përdor një qasje sistematike dhe model të strukturuar për analizimin e faktorëve tipikë të rrezikut, që përfshijnë probabilitetin dhe ndikimin në shërbime në terma të humbjes së ***konfidencialitetit, integritetit dhe/ose disponueshmërisë (CIA)*** të të dhënave dhe/ose një funksioni të një shërbimi kritik dhe të rëndësishëm.

Faktorët e rrezikut përfshijnë, si më poshtë vijon:

- Kërcënimi – Çfarë mund të ndodhë për të dëmtuar dhe/ose ndërprerë funksionimin normal të një shërbimi të caktuar?
- Dobësia – Pikat e dobëta në sistem/arkitekturë, që shfrytëzohen nga vektori i kërcënimit me qëllim keqfunksionimin ose ndërprerjen e tij.
- Probabiliteti/frekuenca (ekspozimi) – Mundësia që kërcënimi të shfrytëzojë dobësinë për të shkaktuar një ndikim negativ.
- Ndikimi/serioziteti i pasojave – Në rast se një kërcënim materializohet, vlerësohet niveli i ashpërsisë së ndikimit të mundshëm që ai mund të ketë mbi funksionimin e shërbimit apo infrastrukturës përkatëse. Ky vlerësim realizohet në mënyrë të kontekstualizuar, duke u mbështetur në të dhënat e mbledhura përmes pyetësorëve, auditimeve dhe burimeve të tjera relevante, si dhe në analizën profesionale të stafit vlerësues. Kjo qasje mundëson fleksibilitet dhe përshtatshmëri me realitetin konkret të çdo sektori apo infrastrukture, duke shmangur kufizimet që do të sillte një vlerësim i bazuar vetëm në skenarë të standardizuar.

Metodologjia analizon këta faktorë rreziku në kontekstin e **burimeve njerëzore, proceseve dhe teknologjisë** për të bërë një përcaktim të rrezikut të sigurisë kibernetike për OIKI/OIRI.

Për të grupuar rreziqet e identifikuara, metodologjia përdor 3 (tri) hendeqet kryesore, si më poshtë:

1. Hendeku në burime njerëzore

- Staf i pamjaftueshëm: Numër i pamjaftueshëm personeli për të identifikuar, vlerësuar dhe menaxhuar në mënyrë efektive rreziqet e sigurisë kibernetike.
- Mungesë njohurish të specializuara: Punonjësit mund të mos kenë njohuritë e nevojshme në menaxhimin e rrezikut, analizën e të dhënave ose sigurinë kibernetike.
- Mungesa e trajnimeve dhe ndërgjegjësimi: Programe të pamjaftueshme trajnimi dhe ndërgjegjësimi për punonjësit që të përballojnë rreziqet e sigurisë kibernetike.

2. Hendeku në procese

2.1. Hendeku operacional. Këto janë mangësi në proceset ose praktikat që lidhen me menaxhimin dhe mbrojtjen e sistemeve të informacionit dhe të dhënave. Shembujt përfshijnë plane të pamjaftueshme për përgjigjen ndaj incidenteve, mungesën e auditimeve të rregullta të

sigurisë, mungesën e testimeve periodike të përputhshmërisë dhe penetrimit, dështimin për të zbatuar në mënyrë të vazhdueshme politikat e sigurisë, azhurnimet e pamjaftueshme të sigurisë dhe ndreqjen e cenueshmërive të njohura të *software*-it, dështimin për të rishikuar e vepruar mbi inteligjencën e kërcënimeve, zbutjen/riparimin e cenueshmërive të zbuluara gjatë testimeve etj.

2.2. Hendeku i menaxhimit. I referohet mungesës së një kuadri të qartë dhe të dokumentuar për menaxhimin e rrezikut kibernetik, duke përfshirë edhe mungesën e mekanizmave të brendshëm për vendimmarrje strategjike në lidhje me këto rreziqe. Ky hendek nuk ka të bëjë me përmbajtjen e prioriteteve specifike të operatorit, të cilat mbeten përgjegjësi ekskluzive e tij, por lidhet me ekzistencën ose mungesën e një qasjeje të strukturuar për menaxhimin e tyre.

2.3 Hendeku i politikave dhe përputhshmërisë. Këto ndodhin kur një operator infrastrukture dështon në përmbushjen e kërkesave rregullatore ose standardet e industrisë për mbrojtjen e të dhënave dhe sigurisë së informacionit. Kjo mund të jetë për shkak të politikave të vjetruara, mungesës së ndërgjegjësimit për ndryshimet rregullatore, kontrolleve të pamjaftueshme për të siguruar përputhshmëri me standardet ose dështimit për të përmbushur planin e trajtimit të rrezikut.

3. Hendeku në teknologji

Hendeku teknologjik ndodh kur ka mungesë të zgjidhjeve të nevojshme teknologjike për t'u mbrojtur kundër kërcënimeve kibernetike aktuale dhe të reja. Kjo mund të përfshijë sisteme sigurie të vjetruara, mungesë të mjeteve të avancuara për zbulimin e kërcënimeve, karakteristika të pamjaftueshme të sigurisë në infrastrukturën ekzistuese të IT-së ose dështim për të përdorur praktikat më të mira si "mbrojtja në thellësi", ndarja e rrjeteve në rrjete publike dhe private etj.

Për secilën nga kategoritë e mësipërme janë identifikuar rreziqet shoqëruese si pjesë përbërëse e tyre, ndërsa në tabelën e vlerësimit të rreziqeve janë përcaktuar, gjithashtu, dhe komponentët e triadës CIA, që preken (konfidencialiteti, integriteti dhe disponueshmëria) për çdo gjetje që derivon në rrezik.

Për qëllime të kësaj metodologjie, rreziku do të matet në terma të mundësisë së ndodhjes dhe ndikimi, pra, mundësia që një ngjarje të ndodhë në kombinim me pasojën e saj.

Vlerësimi i mundësisë së ndodhjes: Një vlerë numerike, e cila përfaqëson probabilitetin e një rreziku që të ndodhë. Kjo vlerë përcaktohet nga 1 deri në 5, ku 1 përfaqëson një probabilitet shumë të ulët dhe 5 një probabilitet shumë të lartë të ndodhjes së ngjarjes.

Vlerësimi i ndikimit: Një vlerë numerike, e cila përfaqëson ndikimin e rrezikut, nëse ai ndodh, në terma financiarë, shëndetësorë, mjedisorë etj. Po ashtu, kjo vlerë përcaktohet nga 1 deri në 5, ku 1 përfaqëson një ndikim të papërfillshëm dhe 5 një ndikim kritik ose tepër të lartë.

Llogaritja e vlerës së rrezikut do të jetë prodhimi i vlerës së mundësisë së ndodhjes dhe ndikimit, që do të llogaritet sipas formulës së mëposhtme:

Vlera e Rrezikut = Mundësia e Ndodhjes * Ndikim

12.1 Mundësia e ndodhjes

Mundësia e ndodhjes mbështetet në probabilitetin që një ngjarje të materializohet. Në vijim, faktorët kyçë, që do të konsiderohen në vlerësimin e mundësisë së ndodhjes, përfshijnë, por nuk limitohen në:

- arkitekturën dhe mjedisin e sistemit të informacionit;
- qasjen në sisteme, qëndrueshmërinë kibernetike, forcën dhe natyrën e kërcënimit;
- dobësitë dhe efektivitetin e kontrolleve ekzistuese etj.

Bazuar në mundësinë e ndodhjes, më poshtë është përcaktuar tabela nr. 2 e vlerësimit të probabilitetit të ndodhjes së rreziqeve të ndara në 5 kategori (shumë i ulët (1), i ulët (2), mesatar (3), i lartë (4) dhe shumë i lartë (5)), nëpërmjet mundësisë së materializimit të rrezikut në terma kohorë.

Tabela nr. 2 Mundësia e ndodhjes sipas shpeshtësisë së pritshme të ndodhjes së rrezikut

Mundësia e ndodhjes	Përshkrimi
1	vjetore
2	3-mujore (2–4 herë në vit)
3	mujore (5–12 herë në vit)
4	javore (13–52 herë në vit)
5	ditore (>52 herë në vit)

Tabela nr. 3 prezanton mundësinë e ndodhjes sipas kategorive në terma të triadës së të dhënave CIA.

Tabela nr. 3 Mundësia e ndodhjes sipas kategorive nga 1 deri në 5 dhe triada e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave në total dhe sipas komponentëve përkatës

Kategorizimi		CIA	Konfidencialiteti	Integriteti	Disponueshmeria
1	**Shumë i ulët**	Ka një mundësi shumë të ulët që një kërcënim të materializohet dhe të ndikojë në triadën CIA.	Është shumë e ulët mundësia që informacioni sensitiv të zbulohet në mënyrë të paautorizuar. Proceset dhe teknologjitë e avancuara operojnë efektivisht për të mbrojtur të dhënat.	Është shumë e ulët mundësia që informacioni sensitiv të modifikohet në mënyrë të paautorizuar, falë mekanizmave të fortë të kontrollit të aksesit dhe auditimit.	Është shumë e ulët mundësia që informacioni sensitiv të bëhet i padisponueshëm, si pasojë e marrjes së masave të forta kompensuese.
2	**I ulët**	Ka një mundësi relativisht të ulët që një kërcënim të materializohet dhe të ndikojë në triadën CIA.	Ekziston një probabilitet i ulët që të dhënat konfidenciale të zbulohen, por masat mbrojtëse janë relativisht të mjaftueshme për të parandaluar shumicën e sulmeve.	Ekziston një probabilitet i ulët që të dhënat të komprometohen, por ka kontrolle dhe masa korrigjuese për të zbuluar dhe për të korrigjuar shpejt modifikimet e paautorizuara.	Ekziston një probabilitet i ulët që një sistem të bëhet i padisponueshëm, por procedurat e mirëmbajtjes dhe të testimit të rregullt ndihmojnë në minimizimin e këtij rreziku.
3	**Mesatar**	Kërcënimet janë të mundshme dhe mund të ndodhin nëse nuk zbatohen masa mbrojtëse.	Është e mundur që informacioni konfidencial të zbulohet pa autorizim, nëse sulmuesit shfrytëzojnë dobësitë e njohura/panjohura. Masat mbrojtëse janë implementuar, por ka nevojë për përmirësime të vazhdueshme.	Ekziston një probabilitet mesatar që të dhënat të ndryshohen në mënyrë të paautorizuar, veçanërisht nëse sulmuesit kanë qasje të brendshme ose shfrytëzojnë dobësitë e sistemit.	Është e mundur që një sistem të bëhet i padisponueshëm, për shkak të ndonjë dështimi teknik.
4	**I lartë**	Kërcënimet janë të mundshme dhe pritet të ndodhin nëse nuk ndërmerren masa parandaluese.	Është e mundshme që të dhënat konfidenciale të ekspozohen për shkak të një sërë faktorësh, përfshirë sulmet e sofistikuara ose dobësitë e brendshme të sistemit. Masat mbrojtëse nuk janë implementuar efektivisht.	Është e mundshme që të dhënat të ndryshohen pa autorizim, veçanërisht dhe vihet re mungesë e implementimit efektiv të masave të kontrollit të aksesit dhe monitorimit të vazhdueshëm.	Ekziston një probabilitet i lartë që një sistem të bëhet i padisponueshëm, për shkak të sulmeve të vazhdueshme ose dështimeve teknike të pajisjeve.
5	**Shumë i lartë**	Kërcënimet janë potencialisht të sigurta që do të ndodhin dhe do të ndikojnë në triadën CIA.	Është pothuajse e sigurt që të dhënat konfidenciale të ekspozohen, nëse nuk merren masa mbrojtëse urgjente dhe të efektshme, sidomos në rastet e sulmeve të sofistikuara	Është pothuajse e sigurt që të dhënat do të ndryshohen pa autorizim, për shkak të mungesës së plotë të kontrolleve të aksesit dhe monitorimit.	Është pothuajse e sigurt që një sistem të bëhet i padisponueshëm për një periudhë të konsiderueshme kohe, veçanërisht nëse ka sulme të sofistikuara që shfrytëzojnë dobësitë e njohura/panjohura ose mungesën e mbrojtjeve të duhura.

12.2. Ndikimi

Vlerësimi i ndikimit do të kryhet bazuar në analizimin e ndikimit, që do të sillte në sigurinë kibernetike të infrastrukturës në hendekun në kapacitetet teknike, procese dhe burime njerëzore, si dhe peshat specifike të përcaktuara për çdo kategori, sipas pyetësorëve që do të dërgohen pranë OIKI-t/OIRI-t nga AKSK-ja të kësaj metodologjie.

Tabela nr. 4 prezanton ndikimin (impaktin) sipas kategorive në terma të triadës së të dhënave: konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave.

Tabela nr. 4 Mundësia e ndikimit sipas kategorive nga 1 deri në 5 dhe triada e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave në total dhe sipas komponentëve përkatës

Kategorizimi		CIA	Konfidencialiteti	Integriteti	Disponueshmëria
1	Shumë i ulët	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij, si dhe ndërprerja e aksesit/përdorimit të sistemeve/rrjeteve teknologjike të informacionit pritet të ketë një ndikim të papërfillshëm për organizatën/kompaninë. Efektet janë lehtësisht të menaxhueshme dhe nuk ka pritshmëri për të shkaktuar dëme ose ndërprerje të shërbimit të ofruar.	Një shkelje e papërfillshme e konfidencialitetit që nuk ndikon të dhënat. Nuk ka efekt, as pasoja për organizatën ose individët.	Ndryshime të papërfillshme dhe të parëndësishme në të dhëna josensitive dhe që nuk ndikojnë në operacione. Nuk ka efekt, as pasoja për organizatën ose individët.	Ndërprerje e vogël ose e parëndësishme, që nuk ndikon në funksionet kritike të biznesit ose shërbimet kryesore. Shërbimi rikthehet shpejt pa ndikime të rëndësishme.
2	I ulët	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij, si dhe ndërprerja e aksesit/përdorimit të sistemeve/rrjeteve teknologjike të informacionit pritet të ketë një ndikim të ulët për organizatën/kompaninë. Efektet janë të limituara dhe të menaxhueshme me burimet dhe procedurat ekzistuese për vazhdimësinë e ofrimit të shërbimit.	Një shkelje e papërfillshme e konfidencialitetit, që nuk ndikon të dhënat sensitive. Efekti është minimal dhe nuk ka pasoja për organizatën ose individët.	Ndryshime në të dhëna josensitive dhe që nuk ndikojnë në operacionet. Nuk ka efekt, as pasoja për organizatën ose individët.	Ndërprerje e shërbimit që ndikon në funksionet jokritike. Shërbimi rikthehet brenda një periudhe të shkurtër kohore me pasoja minimale.
3	Moderuar	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij, si dhe ndërprerja e aksesit/përdorimit të sistemeve/rrjeteve teknologjike të informacionit pritet të ketë një ndikim të moderuar për organizatën/kompaninë. Efektet në këtë kategori kanë potencialin për të shkaktuar ndërprerje të shërbimeve dhe nëse nuk ndërmerren masa për minimizimin ose eliminimin e tyre.	Shkelje që ndikon në një sasi të dhënash të ndjeshme me efekt të kufizuar. Ekspozimi mund të ketë pasoja negative për individët ose organizatën dhe kërkon masa korrigjuese.	Ndryshime në të dhëna sensitive, që ndikojnë lehtësisht në operacione. Korrigjimi kërkon kohë dhe burime.	Ndërprerje që ndikon në disa funksione kritike. Rimëkëmbja kërkon kohë dhe përpjekje të konsiderueshme me pasoja të moderuara për organizatën.
4	I lartë	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij, si dhe ndërprerja e aksesit/përdorimit të sistemeve/rrjeteve teknologjike të informacionit	Një shkelje e rëndësishme që ndikon në një sasi relativisht të madhe të të dhënave sensitive.	Ndryshime të mëdha në të dhëna sensitive, që ndikojnë në operacione dhe	Ndërprerje e rëndësishme, që ndikon në shumicën e funksioneve kritike. Rimëkëmbja

		pritet të ketë një ndikim serioz, të lartë për organizatën/kompaninë. Efektet janë të konsiderueshme dhe mund të shkaktojnë ndërprerje të rëndësishme të shërbimit nëse nuk trajtohen brenda një kohe të shkurtër dhe nuk merren masat e duhura në ruajtjen e vazhdimësisë së shërbimit të ofruar.	Pasojat janë të gjera dhe mund të përfshijnë humbje të mëdha financiare ose dëmtim të reputacionit.	vendimmarrje. Korrigjimi kërkon përpjekje të mëdha në kohë dhe burime.	është e komplikuar dhe kërkon burime të mëdha, me pasoja të rënda për organizatën.
5	Shumë i lartë/kritik	Zbulimi i paautorizuar i informacionit, modifikimi, prishja e tij, si dhe ndërprerja e aksesit/përdorimit të sistemeve/rrjeteve teknologjike të informacionit pritet të ketë një ndikim jashtëzakonisht të rëndë, kritikë për organizatën/kompaninë. Efektet e ndikimit janë në nivelin më të lartë dhe kërkojnë vëmendje të menjëhershme. Ekziston potenciali shumë i lartë për dëme serioze, të pariparueshme, duke rrezikuar vazhdimësinë e punës dhe ofrimin e shërbimit përtej kohës së toleruar.	Një shkelje shumë e rëndë që ndikon në një sasi të konsiderueshme të dhënash sensitive. Pasojat janë katastrofike, duke përfshirë humbje të mëdha financiare, dëmtim të reputacionit dhe pasoja ligjore.	Ndryshime thelbësore në të dhënat sensitive që kompromentojnë rëndë operacionet dhe vendimmarrjen. Pasojat janë katastrofike dhe kërkojnë përpjekje të gjera për rikuperim dhe korrigjim.	Ndërprerje shumë e rëndë që ndikon në të gjitha funksionet kritike. Rimëkëmbja është jashtëzakonisht e komplikuar dhe kërkon burime të jashtëzakonshme, me pasoja katastrofike për organizatën.

12.3 Vlerësimi i rrezikut

Qëllimi i një matrice rreziku, e cila kombinon mundësinë e ndodhjes dhe ndikimin në një metrikë të vetme (mundësi e ndodhjes * ndikim), është vlerësimi dhe prioritizimi i rreziqeve në mënyrë efektive.

Qëllimi i vlerësimit të rrezikut është prioritizimi i rreziqeve dhe vendimmarrja se cilat rreziqe mund të pranohen dhe cilat duhet të trajtohen. Rreziku, i cili, nga prodhimi i mundësisë së ndodhjes dhe ndikimi, do të klasifikohet si "shumë i ulët" dhe "i ulët", do të konsiderohet si rrezik i pranuar nga AKSK-ja, ndërsa për kategoritë e tjera të rrezikut, infrastrukturat e rëndësishme dhe kritike të informacionit janë përgjegjëse për përcaktimin e planit të trajtimit dhe zbutjes, duke u bazuar në metodologjitë përkatëse të operatorëve.

Matrica në tabelën 5 tregon klasifikimet e rrezikut, ku zonat jeshile tregojnë se rreziku është në pragun e pranueshëm, zonat e verdhë, portokalli dhe e kuqe tregojnë se një rrezik nuk përmbush kriteret e pranimit nga AKSK-ja dhe, si rrjedhojë, duhet trajtuar me masat përkatëse për zbutjen e tij. Tabela nr. 6 prezanton prioritizimin e trajtimit sipas matricës së rrezikut.

Tabela nr. 5 Prodhimi sasior i mundësisë së ndodhjes dhe ndikimit

Rreziku = Mundësia e ndodhjes * Ndikim

MUNDËSIA		NDIKIMI				
		Shumë i ulët (1)	**I ulët (2)**	**Mesatar (3)**	**I lartë (4)**	**Shumë i lartë (5)**
	Shumë i ulët (1)	1	2	3	4	5
	I ulët (2)	2	4	6	8	10
	Mesatar (3)	3	6	9	12	15
	I lartë (4)	4	8	12	16	20
	Shumë i lartë (5)	5	10	15	20	25

Rreziqet do të prioritizohen për trajtim nga OIKI/OIRI, sipas prodhimit sasior dhe klasifikimit të tyre, në mënyrë që rreziqet me prodhim sasior **"I lartë"** apo "**Shumë i lartë**" rekomandohen të trajtohen para rreziqeve me nivele më të ulëta për operatorët e infrastrukturave.

Tabela nr. 6 Prioritizimi i trajtimit sipas matricës së rrezikut

Vlera e rrezikut	Niveli i rrezikut	Koha e trajtimit
[1-3]	**Shumë i ulët**	**Nuk ka nevojë për trajtim**
[4-6]	**E ulët**	**Nuk ka nevojë për trajtim**
[7-11]	**Mesatar**	**Ka nevojë për trajtim deri në 12 muaj**
[12-19]	**I Lartë**	**Ka nevojë për trajtim deri në 6 muaj**
[20-25]	**Shume i lartë**	**Ka nevojë për trajtim deri në 3 muaj**