LIGJ
Nr. 25/2024

PËR SIGURINË KIBERNETIKE[1]

Në mbështetje të neneve 78, 81, pika 1, dhe 83, pika 1, të Kushtetutës, me propozimin e Këshillit të Ministrave,

KUVENDI
I REPUBLIKËS SË SHQIPËRISË

VENDOSI:

KREU I

DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti i ligjit

1. Objekti i këtij ligji është përcaktimi i të drejtave dhe detyrimeve të subjekteve publike dhe private, të cilat administrojnë infrastruktura të informacionit, rrjetet e komunikimit dhe sistemet e tyre, cenimi apo shkatërrimi i të cilave do të kishte impakt në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.

2. Ky ligj gjithashtu përcakton:

a) autoritetin përgjegjës për sigurinë kibernetike në Republikën e Shqipërisë, i cili është edhe pika e vetme e kontaktit për çështje të sigurisë kibernetike, si dhe institucionet e tjera përgjegjëse të sigurisë dhe mbrojtjes, që ndërveprojnë për çështjet e sigurisë kibernetike në vend;

b) ekipet e përgjigjes ndaj incidenteve të sigurisë kibernetike, si: CSIRT-in Kombëtar, CERT-in, CSIRT-et sektoriale;

c) autoritetin përgjegjës për hartimin e Strategjisë Kombëtare të Sigurisë Kibernetike;

ç) masat e sigurisë kibernetike dhe masat e menaxhimit të rrezikut të sigurisë kibernetike, të cilat janë të detyrueshme për zbatim nga subjektet e përmendura në anekset I dhe II të këtij ligji;

d) detyrimin për raportimin e incidenteve të sigurisë kibernetike nga subjektet e përmendura në anekset I dhe II të këtij ligji;

dh) rregullat dhe detyrimet për ndarjen e informacionit të sigurisë kibernetike.

Neni 2
Qëllimi i ligjit

Qëllimi i këtij ligji është përcaktimi i masave të sigurisë me qëllim arritjen e një niveli të lartë të sigurisë kibernetike për rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë.

Neni 3
Fusha e zbatimit

Dispozitat e këtij ligji zbatohen për të gjitha subjektet publike dhe private, që administrojnë sisteme dhe rrjete të informacionit, sipas përcaktimeve të bëra në anekset I dhe II të këtij ligji.

---

[1] Ky ligj është përafruar pjesërisht me direktivën (BE) nr. 2022/2555, të Parlamentit dhe Këshillit, datë 14 dhjetor 2022, "Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, e cila ka ndryshuar rregulloren (BE) nr. 910/2014 dhe direktivën (BE) nr. 2018/1972, si dhe ka shfuqizuar direktivën (BE) nr. 2016/1148. Numri CELEX 32022L2555, Fletorja Zyrtare e Bashkimit Evropian, seria L, nr. 333, datë 27.12.2022, faqe 80–152.

Neni 4
Parime të përgjithshme të sigurisë kibernetike

1. Përpunimi i të dhënave personale kryhet në përputhje me dispozitat e përcaktuara në legjislacionin në fuqi për mbrojtjen e të dhënave personale.

2. Në përputhje me përcaktimet e bëra në këtë ligj, zbatohet për aq sa është e mundur parimi i neutralitetit të teknologjisë, sipas të cilit subjektet e këtij ligji janë të lira për të zgjedhur teknologjinë më të përshtatshme për nevojat e tyre duke mos imponuar dhe as diskriminuar ndonjë lloj të veçantë teknologjie, duke inkurajuar përdorimin e standardeve evropiane dhe ndërkombëtare dhe specifikimeve teknike të rëndësishme për sigurinë e rrjetit dhe sistemeve të informacionit.

Neni 5
Përkufizime

Në kuptim të këtij ligji, termat e mëposhtëm kanë këto kuptime:

1. "Autoriteti përgjegjës për sigurinë kibernetike" është Autoriteti Kombëtar për Sigurinë Kibernetike, organi publik përgjegjës për zbatimin dhe mbikëqyrjen e këtij ligji, në vijim Autoriteti.

2. "Akreditim" sipas këtij ligji ka të njëjtin kuptim me përkufizimin e dhënë në legjislacionin në fuqi për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë.

3. "CERT" është Ekipi i Përgjigjes ndaj Emergjencave të Sigurisë Kibernetike pranë Autoritetit.

4. "CSIRT Kombëtar" është Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike pranë Autoritetit.

5. "CSIRT sektorial" është personi apo ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike për sektorin përkatës, sipas përcaktimeve në anekset e këtij ligji, i vendosur pranë një operatori që administron infrastruktura kritike dhe të rëndësishme të informacionit ose institucionit përgjegjës të linjës.

6. "CSIRT qeveritar" është CSIRT-i sektorial, i cili menaxhon të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit për sektorin qeveritar.

7. "CSIRT pranë operatorëve" është ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike, pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.

8. "Certifikatë e sigurisë kibernetike" është një dokument i lëshuar nga një organ i vlerësimit të konformitetit për sigurinë kibernetike, që vërteton se një produkt, shërbim ose proces TIK është vlerësuar për pajtueshmërinë me kërkesat specifike të sigurisë, të përcaktuara në skemën e certifikimit të sigurisë kibernetike.

9. "ENISA" është Agjencia për Sigurinë Kibernetike e Bashkimit Evropian.

10. "Emergjencë e sigurisë kibernetike" është situata gjatë së cilës siguria e informacionit në sistemet e informacionit ose siguria e rrjeteve të komunikimeve elektronike është cenuar duke vënë në rrezik interesin publik të Republikës së Shqipërisë.

11. "Grupi i bashkëpunimit" është një organ i krijuar nga direktiva (BE) nr. 2022/2555 e Parlamentit dhe Këshillit Evropian, datë 14 dhjetor 2022, me qëllimin për të mbështetur e lehtësuar bashkëpunimin strategjik dhe shkëmbimin e informacionit midis shteteve anëtare të BE-së.

12. "Hapësirë kibernetike" është mjedisi digjital i aftë të krijojë, të procesojë dhe të shkëmbejë komunikimin elektronik të informacionit të krijuar nga rrjetet dhe sistemet e informacionit edhe pa qenë të lidhur në internet.

13. "Incident i sigurisë kibernetike" është çdo ngjarje që komprometon disponueshmërinë, vërtetësinë, integritetin, konfidencialitetin e të dhënave të ruajtura, të transmetuara apo të përpunuara ose të shërbimeve të ofruara apo të aksesueshme përmes rrjeteve dhe sistemeve të informacionit.

14. "Infrastrukturë kritike e informacionit" është tërësia e rrjeteve dhe sistemeve të informacionit, të zotëruara nga një autoritet publik ose privat, që ofrojnë shërbime, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.

15. "Infrastrukturë e rëndësishme e informacionit" është tërësia e rrjeteve dhe sistemeve të informacionit të zotëruara nga një autoritet publik ose privat, i cili nuk është pjesë e infrastrukturës kritike

të informacionit, por që mund të rrezikojë apo të kufizojë ofrimin e shërbimit dhe vazhdimësinë e punës, në rastin e cenimit të sigurisë së informacionit.

16. "Kërcënim kibernetik" është një ngjarje ose veprim i mundshëm, që mund të dëmtojë, të ndërpresë ose të ndikojë negativisht në rrjetet e sistemet e informacionit për përdoruesit e tyre dhe persona të tjerë.

17. "Krizë kibernetike" është situata gjatë së cilës siguria e informacionit në sistemet e informacionit ose siguria e rrjeteve të komunikimeve elektronike është seriozisht e rrezikuar, duke vënë në rrezik interesin publik të Republikës së Shqipërisë.

18. "Log-e" është mesazh apo e dhënë mbi ngjarje lidhur me sigurinë kibernetike.

19. "Masat e sigurisë kibernetike" janë tërësia e veprimeve për rritjen e sigurisë së informacionit në sistemet e informacionit dhe disponueshmëria e besueshmëria e shërbimeve të rrjeteve të komunikimit në hapësirën kibernetike.

20. "Motor kërkimi në internet" është një shërbim digjital që lejon përdoruesit të vendosin pyetje për të kryer kërkime në parim në të gjitha faqet e internetit ose në të gjitha faqet e internetit në një gjuhë të caktuar, në bazë të një pyetjeje për çdo temë në formën e një fjalëkyçi, kërkese zanore, fraze ose hyrjeje tjetër dhe rezultatet e kthimit në çdo format në të cilin mund të gjenden informacionet në lidhje me përmbajtjen e kërkuar.

21. "Operator i infrastrukturës kritike të informacionit" është çdo person fizik ose juridik, i cili administron infrastrukturën kritike të informacionit dhe plotëson kërkesat e përcaktuara në këtë ligj.

22. "Operator i infrastrukturës së rëndësishme të informacionit" është çdo person fizik ose juridik, i cili administron infrastrukturën e rëndësishme të informacionit dhe plotëson kërkesat e përcaktuara në këtë ligj.

23. "Organe të vlerësimit të konformitetit për sigurinë kibernetike" janë personat juridikë kombëtarë ose ndërkombëtarë, të akredituar nga institucioni përgjegjës për akreditimin për të kryer vlerësimet dhe konformitetin e produkteve, shërbimeve dhe proceseve që lidhen me sigurinë kibernetike në TIK, si dhe vlerësimin e masave të sigurisë kibernetike të implementuara nga infrastrukturat kritike dhe të rëndësishme të informacionit.

24. "Ofruesi i shërbimit DNS" është një ent, i cili ofron:

a) shërbimet rekursive të zgjidhjes së emrave të domenit të disponueshëm publikisht për përdoruesit fundorë të internetit;

b) shërbime autoritative për zgjidhjen e emrave të *domain*-it për përdorim nga palët e treta, me përjashtim të serverave të emrave rrënjë.

25. "Ofrues i shërbimit të menaxhuar" është një ent që ofron shërbime në lidhje me instalimin, menaxhimin, funksionimin ose mirëmbajtjen e produkteve të TIK-ut, rrjeteve, infrastrukturës, aplikacioneve ose çdo rrjeti dhe sistemet e tjera të informacionit, nëpërmjet asistencës ose administrimit aktiv të kryer ose në ambientet e klientëve, ose në distancë.

26. "Ofrues i menaxhuar i shërbimit të sigurisë" është një ofrues shërbimi të menaxhuar, që kryen ose ofron ndihmë për aktivitetet në lidhje me menaxhimin e rrezikut të sigurisë kibernetike.

27. "Organizatë kërkimore" është një subjekt që ka si qëllim parësor të kryejë kërkime zhvillimi të aplikuara ose eksperimentale me synimin për të shfrytëzuar rezultatet e atij kërkimi për qëllime komerciale, por që nuk përfshijnë institucionet arsimore.

28. "Pika e shkëmbimit të internetit" *(internet exchange point)* është një infrastrukturë rrjeti, që lejon ndërlidhjen e më shumë se dy sistemeve autonome të pavarura, kryesisht për të lehtësuar shkëmbimin e trafikut të internetit, siguron ndërlidhje vetëm me sistemet autonome, si dhe nuk kërkon që trafiku i internetit që kalon midis dy sistemeve autonome pjesëmarrëse të kalojë përmes një sistemi të tretë autonom dhe nuk cenon ose ndërhyn në një trafik të tillë.

29. "Playbooks" është një udhërrëfyes, i cili tregon një procedurë të mirëpërcaktuar që duhet të ndiqet për menaxhimin e çdo kategorie incidenti të sigurisë kibernetike.

30. "Produkt TIK" është një element ose një grup elementesh të një rrjeti ose sistemi informacioni.

31. "Procese TIK" janë një grup aktivitetesh që kryejnë projektimin, zhvillimin, ofrimin ose mirëmbajtjen e një produkti ose shërbimi TIK.

32. "Përmbajtje të dëmshme për fëmijën", sipas këtij ligji, ka të njëjtin kuptim me përkufizimin e dhënë në legjislacionin në fuqi për të drejtat dhe mbrojtjen e fëmijës.

33. "Platformë e shërbimeve të rrjeteve sociale" është një platformë që u mundëson përdoruesve fundorë të lidhen, të ndajnë, të zbulojnë dhe të komunikojnë me njëri-tjetrin nëpërmjet pajisjeve të shumta, veçanërisht përmes bisedave, postimeve, videove dhe rekomandimeve.

34. "Regjistri i emrave të *domain*-eve me nivel të lartë.al" ose "regjistri i emrave të *domain*-eve TLD.al" është regjistri me emrat e *domain*-eve të internetit të regjistruar në Republikën e Shqipërisë me prapashtesën ".al", që administrohet nga autoriteti përgjegjës për komunikimet elektronike dhe postare, i cili harton, miraton dhe aplikon një rregullore të veçantë për këtë qëllim. Regjistri përfshin emrat e *domain*-eve (dhe nën*domain*-eve) ccTLD.al, të dhënat e poseduesve të tyre, historikun e veprimeve me *domain*-et me .al dhe sistemin teknik ccTLD.al, i cili përfshin funksionimin e serverave dhe pajisjeve të tjera të nevojshme, mirëmbajtjen e bazave të të dhënave dhe shpërndarjen e skedarëve të zonës TLD për të bërë të mundur aksesimin e emrave të *domain*-eve me .al në internet etj., të cilat përfshihen në rregulloren e sipërpërmendur.

35. "Rrjet dhe sistem i informacionit", është:

a) një rrjet i komunikimeve elektronike, sipas përcaktimeve të bëra në ligjin për komunikimet elektronike në fuqi;

b) çdo pajisje ose grup i pajisjeve të lidhura ose të ndërlidhura dhe një ose disa prej tyre kryejnë përpunimin automatik të të dhënave digjitale nëpërmjet një programi;

c) të dhënat digjitale të ruajtura, të përpunuara, të marra ose të transmetuara nga elemente të parashikuara në shkronjat "a" dhe "b" të kësaj pike, për funksionimin, përdorimin, mbrojtjen dhe mirëmbajtjen e tyre.

36. "Rrezik i sigurisë kibernetike" është një ngjarje e identifikueshme me efekt të mundshëm negativ për sigurinë e rrjeteve e të sistemeve të informacionit.

37. "Rrjeti i CSIRT-eve" është rrjeti i krijuar nga direktiva (BE) nr. 2022/2555 e Parlamentit dhe Këshillit Evropian, datë 14 dhjetor 2022, i përbërë nga CSIRT-et kombëtare të shteteve anëtare të BE-së me qëllimin promovimin e bashkëpunimit operacional të shpejtë dhe efektiv midis tyre.

38. "Rrjeti Evropian i Organizatave Ndërlidhëse të Krizave Kibernetike (EU-CyCLONe)" është rrjeti i krijuar nga direktiva (BE) nr. 2022/2555 e Parlamentit dhe Këshillit Evropian, datë 14 dhjetor 2022, me qëllimin për të mbështetur koordinimin e menaxhimit të incidenteve dhe krizave të sigurisë kibernetike në shkallë të gjerë në nivel operacional dhe për të siguruar shkëmbimin e informacionit ndërmjet shteteve anëtare të BE-së, institucioneve, organeve, zyrave dhe agjencive të BE-së.

39. "Rrjet i shpërndarjes së përmbajtjes" është një rrjet serverash të shpërndarë gjeografikisht, me qëllim sigurimin e disponueshmërisë, aksesueshmërisë ose shpërndarjes së shpejtë të përmbajtjes dhe shërbimeve digjitale për përdoruesit e internetit në emër të përmbajtjes dhe ofruesve të shërbimeve.

40. "Rrjet i komunikimeve publike elektronike" është i njëjtë me përkufizimin e dhënë në legjislacionin në fuqi për komunikimet elektronike.

41. "Qëndrueshmëria kibernetike" është aftësia e sistemeve të informacionit për të mbrojtur të dhënat nga sulmet kibernetike, si dhe aftësia për të rifilluar funksionimin normal të punës brenda një kohe, e cila nuk ndikon në veprimtarinë e operatorit të infrastrukturës kritike ose të rëndësishme të informacionit në rast të një sulmi kibernetik.

42. "Siguria e rrjetit dhe sistemeve të informacionit" është aftësia e rrjetit dhe e sistemeve të informacionit për t'i rezistuar në një nivel të caktuar sigurie çdo veprimi, që komprometon disponueshmërinë, vërtetësinë, integritetin dhe konfidencialitetin e të dhënave të ruajtura, të transmetuara ose të përpunuara dhe shërbimeve përkatëse të ofruara përmes këtij rrjeti ose sistemeve të informacionit.

43. "Siguria kibernetike" është tërësia e veprimeve të nevojshme për të mbrojtur rrjetet dhe sistemet e informacionit, përdoruesit e këtyre rrjeteve dhe sistemeve, si dhe personat e tjerë të prekur nga kërcënimet kibernetike.

44. "Strategjia Kombëtare për Sigurinë Kibernetike" është një dokument politikash që përcakton objektiva, plane dhe prioritete strategjike për sigurinë e rrjeteve dhe sistemeve të informacionit dhe krijimin e hapësirave kibernetike të sigurta për shoqërinë në nivel kombëtar.

45. "Skema e certifikimit të sigurisë kibernetike" është tërësia e rregullave, kërkesave teknike, standardeve dhe procedurave që zbatohen për certifikimin ose vlerësimin e konformitetit të produkteve, shërbimeve dhe proceseve që lidhen me sigurinë kibernetike në TIK.

46. "Standard", sipas këtij ligji, ka të njëjtin kuptim me përkufizimin e dhënë në legjislacionin në fuqi për standardizimin.

47. "Specifikim teknik" është një dokument, i cili përcakton karakteristikat e kërkuara të një produkti, si nivelet e cilësisë, performancës dhe sigurisë, duke përfshirë kërkesat e zbatueshme për produktin në lidhje me emrin me të cilin produkti shitet, terminologjinë, simbolet, metodat e testimit, paketimi, shënjimi ose etiketimi dhe procedurat e vlerësimit të konformitetit. Ky term mbulon gjithashtu metodat dhe proceset e prodhimit.

48. "Sistemi i emrave të *domain*-eve (DNS)" është një sistem që në mënyrë hierarkike shpërndan emërtime dhe mundëson identifikimin e shërbimeve dhe burimeve të internetit, duke lejuar pajisjet e përdoruesit fundor të përdorin shërbimin e rrugëzimit dhe lidhjes në internet për të arritur ato shërbime dhe burime.

49. "Subjektet e tjera përgjegjëse në fushën e sigurisë kibernetike" janë institucionet eprore ose rregullatore përgjegjëse për fushën e veprimtarisë së sektorëve, sipas të cilëve kategorizohen infrastrukturat kritike dhe të rëndësishme të informacionit.

50. "Skanim proaktiv" është kryerja e një ose disa veprimeve paraprake të avancuara, që bëjnë të mundur identifikimin, zbulimin dhe memorizimin e rreziqeve me ndikim të konsiderueshëm përpara shfaqjes së tyre.

51. "Shërbimi digjital" është çdo shërbim i shoqërisë së informacionit, sipas përcaktimeve të bëra në ligjin për tregtinë elektronike.

52. "Shërbim TIK" është një shërbim që konsiston plotësisht ose kryesisht në transmetimin, ruajtjen, marrjen ose përpunimin e informacionit me anë të rrjetit dhe sistemeve të informacionit.

53. "Shërbimet *cloud computing*" është një shërbim digjital që mundëson administrimin sipas kërkesës dhe akses të gjerë në distancë në një grup të shkallëzueshëm dhe elastik të burimeve kompjuterike të ndashme, duke përfshirë vendin, ku burimet e tilla shpërndahen në disa lokacione.

54. "Shërbimi i qendrës së të dhënave" është një shërbim që përfshin struktura ose grupe strukturash, të dedikuara për të centralizuar akomodimin, ndërlidhjen dhe funksionimin e teknologjisë së informacionit dhe pajisjeve të rrjetit që ofrojnë ruajtjen, përpunimin e të dhënave dhe shërbimet e transportit së bashku me të gjitha objektet dhe infrastrukturat për shpërndarjen e energjisë dhe kontrollin mjedisor.

55. "Shërbim i komunikimeve elektronike" është i njëjtë me përkufizimin e dhënë në legjislacionin në fuqi për komunikimet elektronike.

56. "Treg *online*" është një shërbim që përdor *software*, duke përfshirë një faqe interneti, pjesë të një faqeje interneti ose të një aplikacioni, i operuar nga ose në emër të një tregtari që i lejon konsumatorët të përfundojnë në distancë kontrata me tregtarë ose konsumatorë të tjerë.

57. "Trajtimi i incidentit të sigurisë kibernetike" janë të gjitha procedurat e nevojshme për parandalimin, identifikimin, analizimin, reagimin dhe rikuperimin ndaj një incidenti të sigurisë kibernetike.

58. "Vulnerabilitet" është një dobësi, ndjeshmëri ose defekt i produkteve ose shërbimeve TIK, që mund të shfrytëzohet nga një kërcënim kibernetik.

KREU II
ORGANIZIMI INSTITUCIONAL DHE SUBJEKTET PËRGJEGJËSE PËR SIGURINË KIBERNETIKE

Neni 6
Strategjia Kombëtare për Sigurinë Kibernetike

1. Autoriteti është institucioni përgjegjës për hartimin dhe monitorimin e zbatimit të Strategjisë Kombëtare për Sigurinë Kibernetike, i cili koordinon punën me institucionet e tjera përgjegjëse për sigurinë kibernetike.

2. Në Strategjinë Kombëtare të Sigurisë Kibernetike përcaktohen:

a) objektivat dhe prioritetet e strategjisë së sigurisë kibernetike për sektorët e përmendur në anekset I dhe II të këtij ligji;

b) kuadri ligjor për të arritur objektivat dhe prioritetet e përmendura në shkronjën "a" të pikës 2 të këtij neni, si dhe politikat e përmendura në pikën 3 të këtij neni;

c) kuadri ligjor, që përcakton rolet dhe përgjegjësitë e aktorëve përkatës në nivel kombëtar, duke mbështetur bashkëpunimin dhe koordinimin në nivel kombëtar ndërmjet autoriteteve kompetente, pikën e vetme të kontaktit dhe CSIRT-eve sipas këtij ligji, si dhe koordinimin e bashkëpunimin ndërkombëtar;

ç) programet e trajnimit, ndërgjegjësimit dhe edukimit;

d) masat që sigurojnë gatishmërinë, reagimin dhe rikuperimin nga incidentet, duke përfshirë bashkëpunimin ndërmjet sektorit publik e privat;

dh) një plan i identifikimit të aseteve lidhur me sigurinë kibernetike dhe vlerësimin e rrezikut të sigurisë kibernetike;

e) lista e aktorëve të ndryshëm që do të përfshihen në zbatimin e strategjisë.

3. Strategjia përmban në veçanti politikat e mëposhtme:

a) adresimin e sigurisë kibernetike në zinxhirin e furnizimit për produktet TIK dhe shërbimet TIK që përdoren nga subjektet për ofrimin e shërbimeve të tyre;

b) menaxhimin e vulnerabiliteteve, duke përfshirë promovimin dhe koordinimin për zbulimin e vulnerabiliteteve;

c) promovimin e zhvillimit dhe të integrimit të teknologjive të avancuara, që synojnë zbatimin e masave moderne të menaxhimit të riskut të sigurisë kibernetike;

ç) promovimin dhe zhvillimin e trajnimeve për sigurinë kibernetike, edukimin, aftësitë në sigurinë kibernetike, ndërgjegjësimin, nisma për kërkim dhe zhvillim, si dhe udhëzime për praktikat dhe kontrollet më të mira të higjienës kibernetike, për qytetarët, palët e interesuara dhe subjektet e këtij ligji;

d) mbështetjen e institucioneve akademike dhe kërkimore për të zhvilluar, përmirësuar dhe promovuar mjetet e sigurisë kibernetike dhe infrastrukturës së rrjetit;

dh) promovimin e mbrojtjes aktive kibernetike.

4. Strategjia Kombëtare e Sigurisë Kibernetike hartohet për një periudhë 5-vjeçare dhe miratohet me vendim të Këshillit të Ministrave.

5. Strategjia shoqërohet nga plani i veprimit, i cili hartohet nga Autoriteti në koordinim me institucionet përgjegjëse të sigurisë kibernetike, për një periudhë të paktën dyvjeçare dhe miratohet me vendim të Këshillit të Ministrave.

Neni 7

Autoriteti përgjegjës për sigurinë kibernetike

1. Autoriteti është organ rregullator përgjegjës për mbikëqyrjen dhe zbatimin e legjislacionit për sigurinë kibernetike në Republikën e Shqipërisë.

2. Autoriteti është një person juridik publik, me seli në Tiranë, në varësi të Kryeministrit, i cili financohet nga buxheti i shtetit dhe burime të tjera të ligjshme.

3. Autoriteti, në marrëdhënie me palët e treta, përfaqësohet nga drejtori i përgjithshëm.

4. Marrëdhëniet e punës së drejtorit të përgjithshëm dhe të punonjësve të Autoritetit rregullohen në bazë të dispozitave të ligjit nr. 7961, datë 12.7.1995, "Kodi i Punës i Republikës së Shqipërisë", i ndryshuar.

5. Drejtori i përgjithshëm dhe nëpunësit e njësive teknike të përmbajtjes së Autoritetit, përveç pagës sipas kategorive të pagës së përcaktuar me vendim të Këshillit të Ministrave, përfitojnë një shtesë për natyrë të veçantë pune në masën deri në 800 000 (tetëqind mijë) lekë në muaj. Masa e shtesës për natyrë të veçantë pune për secilën kategori përcaktohet me vendim të Këshillit të Ministrave.

6. Pjesë e strukturës dhe organikës së Autoritetit Kombëtar për Sigurinë Kibernetike është Qendra Kombëtare Operacionale e Sigurisë Kibernetike, përgjegjëse për monitorimin e sigurisë kibernetike, simulimeve, si dhe përcaktimin e masave shtesë për operatorët e infrastrukturave të informacionit për një reagim sa më të shpejtë dhe efikas ndaj incidenteve apo sulmeve kibernetike.

7. Organizimi dhe funksionimi i Autoritetit miratohen me vendim të Këshillit të Ministrave.

Neni 8

Emërimi, lirimi ose shkarkimi i drejtorit të përgjithshëm

1. Drejtori i përgjithshëm i Autoritetit emërohet, lirohet dhe shkarkohet nga Kryeministri.
2. Drejtori i përgjithshëm i Autoritetit duhet të plotësojë kriteret e mëposhtme:
a) të jetë shtetas shqiptar;
b) të ketë zotësi të plotë për të vepruar;
c) të ketë diplomë të nivelit të shtatë të Kornizës Shqiptare të Kualifikimeve, "Master i shkencave" ose të barasvlershme me të, sipas legjislacionit për arsimin e lartë, në fushën e teknologjive të informacionit dhe komunikimit (ICT) apo inxhinierisë elektronike;
ç) të ketë përvojë pune të paktën 10 vjet në profesion;
d) të shquhet për aftësi profesionale në fushën e sigurisë kibernetike, si dhe të jetë i certifikuar ndërkombëtarisht në këtë fushë;
dh) ndaj tij të mos jetë marrë masa disiplinore e largimit nga puna, që nuk është shuar sipas legjislacionit në fuqi;
e) të mos jetë dënuar me vendim gjyqësor të formës së prerë për kryerjen e një vepre penale;
ë) të mos ketë konflikt interesi në ushtrimin e detyrës, sipas përcaktimeve të bëra në legjislacionin në fuqi për parandalimin e konfliktit të interesave në ushtrimin e funksioneve publike.
3. Drejtori i përgjithshëm i Autoritetit lirohet nga detyra kur:
a) plotësohen kushtet për pensionin e plotë të pleqërisë;
b) deklarohet i paaftë për punë nga komisioni kompetent mjekësor;
c) gjendet në një situatë të vazhdueshme të konfliktit të interesit;
ç) jep dorëheqjen nga detyra.
4. Drejtori i përgjithshëm i Autoritetit shkarkohet nga detyra kur:
a) dënohet me vendim gjyqësor të formës së prerë për kryerjen e një krimi apo për kryerjen e një kundërvajtjeje penale me dashje;
b) nuk përmbushen objektivat strategjikë për shkak të performancës së ulët të tij;
c) kryen shkelje të rënda në detyrë.
5. Konsiderohen shkelje të rënda në detyrë:
a) shkelja e përsëritur e rregullave të etikës, sipas legjislacionit në fuqi;
b) shkelja e rregullave për ruajtjen e informacionit të klasifikuar;
c) ushtrimi i detyrës në kushtet e konfliktit të interesit.

Neni 9
Kompetencat e Autoritetit Kombëtar për Sigurinë Kibernetike

Autoriteti, në përputhje me përcaktimet e bëra në këtë ligj, ushtron kompetencat e mëposhtme:
a) identifikon dhe klasifikon infrastrukturat kritike dhe të rëndësishme të informacionit;
b) vepron si pikë qendrore kontakti në nivel kombëtar dhe ndërkombëtar, si dhe koordinon e bashkërendon punën me institucionet e tjera në fushën e sigurisë kibernetike për zgjidhjen e incidenteve kibernetike;
c) vepron në cilësinë e CSIRT-it Kombëtar dhe CERT-it;
ç) përcakton dhe kontrollon zbatimin e masave të sigurisë kibernetike, që duhet të aplikohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit;
d) bashkëpunon dhe shkëmben informacione të rëndësishme me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me të dhënat në sisteme, kur ato janë të rrezikuara për shkak të një incidenti kibernetik;
dh) asiston operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në menaxhimin e incidenteve kibernetike;
e) kryen monitorim aktiv të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet informacioneve të marra nga platformat e jashtme të ngritura nga Autoriteti ose operatorët e infrastrukturave të informacionit, si dhe nga platformat e brendshme me kërkesë nga operatorët e infrastrukturave të informacionit, me qëllim evidentimin e parandalimin e veprimeve keqdashëse;

ë) vlerëson dhe analizon nivelin e sigurisë kibernetike të sistemeve të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet kontrolleve dhe simulimeve të vazhdueshme, si dhe përcakton masa shtesë për operatorët e infrastrukturave të informacionit për një reagim sa më të shpejtë dhe efikas ndaj incidenteve apo sulmeve kibernetike; Metodologjia për vlerësimin dhe analizimin e sigurisë kibernetike miratohet me vendim të Këshillit të Ministrave;

f) regjistron organet e vlerësimit të konformitetit për sigurinë kibernetike për vlerësimin e masave të sigurisë kibernetike;

g) krijon dhe administron regjistrin e dokumentimit të incidenteve të sigurisë kibernetike;

gj) raporton në mënyrë periodike në lidhje me incidentet kibernetike pranë ENISA-s dhe organizmave të tjerë ndërkombëtarë në kuadër të angazhimeve të Republikës së Shqipërisë për çështjet e sigurisë kibernetike;

h) kryen aktivitete ndërgjegjësimi në fushën e sigurisë kibernetike për të gjitha grupet e shoqërisë;

i) Autoriteti, me urdhër të drejtorit të përgjithshëm dhe në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, zhvillon dhe nxit, sa herë vlerësohet e nevojshme, trajnime për personelin e këtyre operatorëve, në kuadër të përmbushjes me efektivitet të lartë të detyrave;

j) ndërmerr masa të nevojshme, bashkëpunon dhe bashkërendon punën me institucionet përgjegjëse për sigurinë dhe mbrojtjen e fëmijëve dhe të rinjve për krijimin e një mjedisi *online* të sigurt kibernetik në Republikën e Shqipërisë.

Neni 10

Raporti për gjendjen e sigurisë kibernetike

1. Me qëllim vlerësimin e nivelit të sigurisë kibernetike në vend, Autoriteti harton një raport për sigurinë kibernetike për një periudhë njëvjeçare, i cili përmban një vlerësim të:

a) rrezikut të sigurisë kibernetike në vend;

b) kapaciteteve të sigurisë kibernetike në vend;

c) burimeve teknike, financiare dhe njerëzore në dispozicion të infrastrukturave të informacionit, politikave të sigurisë kibernetike, zbatimit të masave mbikëqyrëse;

ç) nivelit të përgjithshëm të ndërgjegjësimit për sigurinë kibernetike dhe higjienës kibernetike midis qytetarëve dhe subjekteve të ligjit;

d) nivelit të rritjes së kapaciteteve të sigurisë kibernetike.

2. Raporti përfshin edhe rekomandime të veçanta të politikave për rritjen e nivelit të sigurisë kibernetike në vend dhe një përmbledhje të gjetjeve për periudhën njëvjeçare.

3. Raporti i hartuar sipas pikave 1 dhe 2 të këtij neni i paraqitet Kryeministrit të Republikës së Shqipërisë brenda datës 31 mars të vitit pasardhës.

Neni 11

Subjektet e tjera përgjegjëse për sigurinë kibernetike

Subjekte të tjera përgjegjëse për sigurinë e rrjeteve dhe sistemeve të informacionit në Republikën e Shqipërisë janë si më poshtë:

a) institucionet përgjegjëse të sigurisë dhe mbrojtjes kibernetike:

i. ministria përgjegjëse për transportin, telekomunikacionin dhe shërbimin postar;

ii. ministria përgjegjëse për rendin dhe sigurinë publike;

iii. ministria përgjegjëse për financën;

iv. ministria përgjegjëse për ekonominë;

v. ministria përgjegjëse për kujdesin shëndetësor;

vi. ministria përgjegjëse për mjedisin, turizmin, mbrojtjen e territorit dhe funksione të tjera të lidhura me të;

vii. ministria përgjegjëse për bujqësinë dhe funksione të tjera të lidhura me të;

viii. Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI);

ix. Policia e Shtetit, institucioni përgjegjës për ruajtjen e rendit e të sigurisë publike;

x. Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP);

xi. institucionet e tjera përgjegjëse për ruajtjen dhe përpunimin e të dhënave qeveritare;

xii. çdo institucion tjetër publik i pavarur që administron infrastruktura të informacionit në kuptim të këtij ligji.

b) subjektet përgjegjëse për ofrimin e shërbimeve të sektorëve, si:

i. subjektet që ofrojnë shërbime në sektorët e energjisë, përfshirë sektorët e energjisë elektrike, gazit, naftës dhe energjisë bërthamore;

ii. subjektet që ofrojnë shërbime në sektorët e transportit ajror, detar, hekurudhor, rrugor postar dhe telekomunikacionit;

iii. subjektet që ofrojnë shërbime në sektorët e ekonomisë, financës, infrastrukturës së tregut financiar, sektorin bankar, si dhe sektorët mikrofinanciarë;

iv. subjektet që ofrojnë shërbime në tregun e siguracioneve, shoqëritë e sigurimit;

v. subjektet që ofrojnë shërbime në sektorët e kujdesit të ndihmës shëndetësore të autorizuar dhe të akreditуar nga autoritetet përgjegjëse;

vi. subjektet që ofrojnë shërbime në sektorët e mjedisit, turizmit, mbrojtjes së territorit dhe autoritetet territoriale përgjegjëse për furnizimin dhe shpërndarjen e ujit të pijshëm;

vii. subjektet që ofrojnë shërbime në sektorët e infrastrukturës digjitale, telekomunikacionit, si dhe shërbimet digjitale;

viii. subjektet që ofrojnë shërbime në sektorin arsimor, në veçanti, kur kryejnë veprimtari kërkimore;

ix. çdo sektor tjetër që ofron shërbime nëpërmjet rrjeteve dhe sistemeve të informacionit objekt i këtij ligji.

Neni 12

Identifikimi i infrastrukturave kritike dhe të rëndësishme të informacionit

1. Autoriteti kryen identifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit në vazhdimësi në bashkëpunim dhe në bashkërendim me subjektet e tjera përgjegjëse për sigurinë kibernetike.

2. Identifikimi i operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, sipas përcaktimeve të bëra në anekset I dhe II të këtij ligji, kryhet mbi bazën e një metodologjie, e cila miratohet me vendim të Këshillit të Ministrave.

3. Kriteret mbi të cilat bazohet identifikimi i infrastrukturave kritike dhe të rëndësishme të informacionit janë si më poshtë:

a) shërbimi i ofruar është kritik ose i rëndësishëm për mirëmbajtjen e aktiviteteve shoqërore dhe ekonomike;

b) ofrimi i atij shërbimi varet nga rrjete të komunikimit elektronik dhe sisteme të informacionit;

c) një incident sjell efekte të rëndësishme shkatërruese në ofrimin e atij shërbimi.

4. Subjektet, të cilat do të identifikohen si infrastruktura kritike apo të rëndësishme të informacionit, kanë detyrimin të raportojnë saktë pranë Autoritetit informacionin e mëposhtëm:

a) emrin e subjektit;

b) adresën;

c) kur është e aplikueshme, sektorin dhe nënsektorin përkatës, sipas përcaktimeve të bëra në anekset I dhe II të këtij ligji;

ç) kur është e aplikueshme, një listë të shteteve ku ata ofrojnë shërbime që bëjnë pjesë në fushën e zbatimit të këtij ligji.

5. Lista e infrastrukturave kritike dhe të rëndësishme të informacionit është konfidenciale, miratohet me vendim të Këshillit të Ministrave dhe përditësohet të paktën një herë në dy vjet.

Neni 13

Detyrat dhe përgjegjësitë e CSIRT-it Kombëtar

Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike pranë Autoritetit përmbush detyrat dhe përgjegjësitë e mëposhtme:

a) komunikon në mënyrë aktive nëpërmjet një infrastrukture komunikimi dhe informacioni të përshtatshme, të sigurt dhe të qëndrueshme, përmes së cilës kryhet shkëmbimi i informacionit me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, me qëllim që të sigurohet vazhdimësia e veprimtarisë së tyre në çdo kohë dhe pa ndërprerje;

b) ndërvepron me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet platformave të dedikuara për shpërndarje të informacionit dhe raportimin e incidenteve kibernetike për menaxhimin dhe trajtimin e tyre;

c) monitoron, analizon dhe menaxhon kërcënimet kibernetike, vulnerabilitetet dhe incidentet në nivel kombëtar dhe ofron asistencë teknike për infrastrukturat kritike dhe të rëndësishme të informacionit, sipas kërkesës nga operatorët e infrastrukturave të informacionit;

ç) vepron në cilësinë e koordinatorit për identifikimin e vulnerabiliteteve në rrjetet dhe sistemet e infrastrukturave të informacionit;

d) monitoron, në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, rrjetet dhe sistemet në infrastrukturat e tyre mbi incidente të sigurisë kibernetike apo sulme kibernetike;

dh) trajton incidentet kibernetike në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese kur dyshon për elemente të krimit kibernetik;

e) paralajmëron, njofton dhe shpërndan informacion pranë infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe subjekteve përgjegjëse në lidhje me rreziqet e mundshme, vulnerabilitetet dhe incidentet kibernetike;

ë) mbledh dhe analizon të dhënat nëpërmjet hetimit digjital dhe ofron analizë dinamike të riskut dhe të incidentit, si dhe kryen ndërgjegjësimin për situatën aktuale të sigurisë kibernetike;

f) siguron ruajtjen e log-eve të incidenteve të evidentuara ose të raportuara për një periudhë të përcaktuar në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit;

g) kryen skanime proaktive të rrjeteve dhe të sistemeve të informacionit të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit me qëllim identifikimin e vulnerabiliteteve me impakt të lartë të mundshëm, duke bërë me dije paraprakisht operatorin e infrastrukturës së informacionit për të gjitha elementet teknike dhe ligjore të kryerjes së këtyre skanimeve;

gj) vlerëson kur infrastruktura është në një situatë me risk të lartë dhe kryen veprime reaktive në bashkëpunim me infrastrukturën pas vënies në dijeni të ndodhjes së incidentit kur shërbimi i ofruar nga infrastruktura ka ndaluar së funksionuari për më shumë se 4 orë. Metodologjia për vlerësimin e riskut të infrastrukturës përcaktohet me udhëzim të drejtorit të përgjithshëm të Autoritetit pas konsultimit me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit;

h) kontrollon zbatimin e masave të sigurisë kibernetike nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit;

i) i përgjigjet çdo infrastrukture, në zbatim të procedurave të sigurisë, për të mbështetur në mënyrë aktive zgjidhjen e incidenteve;

j) analizon dhe përgatit masa të natyrës së veçantë sipas incidentit kibernetik dhe i komunikon ato te CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit;

k) përgatit dhe miraton me urdhër të drejtorit të përgjithshëm të Autoritetit udhëzues, politika dhe rregullore për të harmonizuar dhe përmirësuar procedurat e menaxhimit të incidenteve kibernetike;

l) mban regjistrin elektronik të pikave të kontaktit me të dhënat e përcaktuara në shkronjën "f" të nenit 16 dhe në nenin 18 të këtij ligji;

ll) simulon rrjetet dhe sistemet për të gjetur pikat e dobëta të infrastrukturës, duke njoftuar paraprakisht operatorët;

m) analizon incidentin për të gjetur shkakun e tij, si edhe koordinon aktivitetin me operatorët, CSIRT-et sektoriale, institucionet ndërkombëtare dhe qeveritare kur e shikon të arsyeshme;

n) bashkëpunon me rrjetin e CSIRT-eve ndërkombëtare dhe ofron asistencë të përbashkët të bazuar në kapacitetet dhe kompetencat e tij, për anëtarët, pjesë e këtij rrjeti, sipas kërkesës;

nj) koordinon me Policinë e Shtetit dhe çdo institucion përgjegjës për të ruajtur dhe mundësuar mbledhjen e provave kur dyshon për elemente të krimit kibernetik apo veprave të tjera penale të lidhura me to në infrastrukturat e informacionit.

Neni 14
Zbulimi i vulnerabiliteteve

1. CSIRT-i Kombëtar identifikon, analizon dhe ofron asistencë për operatorët e infrastrukturave të informacionit në rast të një vulnerabiliteti të identifikuar kryesisht apo të raportuar nga operatorët e infrastrukturave të informacionit.

2. CSIRT-i Kombëtar në cilësinë e koordinatorit për zbulimin e vulnerabiliteteve kryen këto detyra:

a) identifikon dhe kontakton me subjektet e interesuara;

b) ndihmon personat fizikë ose juridikë që raportojnë një vulnerabilitet;

c) negocion afatet kohore të zbulimit dhe të menaxhimit të vulnerabiliteteve që prekin shumë subjekte.

3. CSIRT-i Kombëtar në cilësinë e koordinatorit për zbulimin e vulnerabiliteteve siguron marrjen e veprimeve korrekte nga operatorët e infrastrukturave të informacionit në lidhje me vulnerabilitetin e raportuar dhe siguron anonimitetin e operatorit që raporton këtë vulnerabilitet.

4. Kur një vulnerabilitet i raportuar prek infrastrukturat e informacionit të shteteve të tjera, CSIRT-i Kombëtar, kur është e nevojshme, bashkëpunon me CSIRT-të e shteteve të tjera të caktuara si koordinatorë mbi bazën e një marrëveshjeje të lidhur ndërmjet palëve.

5. CSIRT-i Kombëtar zhvillon dhe mirëmban një regjistër të vulnerabiliteteve të konstatuara, i cili përmban të dhënat si më poshtë:

a) informacion që përshkruan vulnerabilitetin;

b) produktet TIK ose shërbimet TIK të prekura dhe nivelin e cenueshmërisë në lidhje me rrethanat në të cilat mund të shfrytëzohet;

c) udhëzime në lidhje me zgjidhjet e dhëna për zbutjen e rreziqeve, që vijnë nga vulnerabilitetet e zbuluara.

Neni 15
CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit

1. Subjektet përgjegjëse për ofrimin e shërbimeve, sipas përcaktimeve të bëra në nenin 11 të këtij ligji, ngrenë në strukturën e vet CSIRT-in sektorial, përgjegjës për incidentet e sigurisë kibernetike.

2. Operatori i infrastrukturës kritike dhe operatori i infrastrukturës së rëndësishme të informacionit ngre në strukturën e vet ekipin e përgjigjes ndaj incidenteve të sigurisë kibernetike, CSIRT-in.

3. CSIRT-et përmbushin kërkesat si më poshtë:

a) sigurojnë një nivel të lartë të disponueshmërisë së kanaleve të tyre të komunikimit, duke shmangur çfarëdolloj dështimi dhe kanë disa mjete për t'u kontaktuar dhe për të kontaktuar palët e tjera në çdo kohë duke specifikuar qartë kanalet e komunikimit, duke i bërë ato të njohura për komunitetin dhe partnerët bashkëpunues;

b) ambientet e tyre dhe sistemet mbështetëse të informacionit janë të vendosura në vende të sigurta;

c) janë të pajisur me një sistem të përshtatshëm për menaxhimin dhe drejtimin e kërkesave, veçanërisht për të lehtësuar dorëzimet në mënyrë që këto të jenë efektive dhe eficiente;

ç) sigurojnë konfidencialitetin dhe besueshmërinë e operacioneve të tyre;

d) kanë personel të mjaftueshëm dhe të trajnuar për të siguruar disponueshmërinë e shërbimeve të tyre në çdo kohë, si dhe për këtë qëllim mund të marrin pjesë në rrjete të bashkëpunimit ndërkombëtar;

dh) janë të pajisur me sisteme shtesë kompensimi për të siguruar vazhdimësinë e shërbimeve të tyre.

4. Rregullat teknike të funksionimit të CSIRT-eve pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit dhe CSIRT-eve sektoriale përcaktohen në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit.

5. Mënyra e ngritjes e CSIRT-eve sektoriale përcaktohet me vendim të Këshillit të Ministrave.

Neni 16
Detyrat e CSIRT-it sektorial

Ekipi i Përgjigjes për Incidentet e Sigurisë Kibernetike në Infrastrukturat Kritike dhe të rëndësishme të informacionit, CSIRT-i sektorial, kryen këto detyra:

a) bashkëpunon me Autoritetin për identifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit në Republikën e Shqipërisë;

b) bashkërendon punën me CSIRT-in kombëtar për rritjen e nivelit të sigurisë kibernetike në infrastrukturat kritike dhe të rëndësishme të informacionit që administrojnë operatorët përkatës, sipas fushës së tyre të veprimtarisë;

c) mban përgjegjësi për raportimin e incidenteve kibernetike të ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit, që administrohen prej tyre dhe nga operatorët, sipas fushës së veprimtarisë së tyre;

ç) ruan log-e të incidenteve të evidentuara ose të raportuara për një periudhë të përcaktuar në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit;

d) koordinon me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit për mbrojtjen nga incidentet e sigurisë kibernetike të sistemeve dhe të rrjeteve që ato administrojnë;

dh) njofton CSIRT-in Kombëtar menjëherë pasi identifikon incidentin, si dhe e njofton këtë të fundit në rast të zgjidhjes së shpejtë të incidentit të ndodhur në infrastrukturat që administrojnë;

e) sipas rastit, siguron ndihmë për operatorët e infrastrukturave të informacionit, si dhe u vë në dispozicion informacionin e nevojshëm që mund të lehtësojë trajtimin efektiv të incidentit;

ë) siguron rritje të kapaciteteve të stafit nëpërmjet trajnimeve dhe certifikimeve periodike sipas sektorëve që mbulojnë;

f) cakton pikën e kontaktit e raporton pranë CSIRT-it Kombëtar, si dhe lajmëron për çdo ndryshim të ndodhur brenda 7 ditëve kalendarike;

g) bashkëpunon me palët e interesuara në sektorin privat, me qëllim përmbushjen e objektivave të këtij ligji;

gj) zbaton politikat e sigurisë kibernetike në nivel sektorial.

Neni 17
Detyrat e CSIRT-it pranë operatorëve të infrastrukturave kritike të informacionit dhe të rëndësishme të informacionit

1. Operatori i infrastrukturës kritike të informacionit ngre në strukturën e vet Ekipin e Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike, CSIRT-in.

2. Operatori i infrastrukturës së rëndësishme të informacionit përfshin në strukturën e tij personin përgjegjës për reagimin ndaj incidenteve të sigurisë kibernetike.

3. CSIRT-i pranë operatorëve kryen këto detyra:

a) monitoron rrjetet dhe sistemet e informacionit në infrastrukturën e tyre kritike ose të rëndësishme të informacionit mbi incidente të sigurisë kibernetike apo sulme të mundshme kibernetike;

b) identifikon dhe kategorizon incidentin, si dhe vlerëson shtrirjen dhe dëmin e shkaktuar prej tij;

c) trajton incidentin dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese kur dyshon për elemente të krimit kibernetik apo veprave të tjera penale të lidhura me të;

ç) parandalon incidente të ngjashme në të ardhmen duke marrë masa parandaluese;

d) përgatit dhe dërgon pranë CSIRT-it Kombëtar raportet e incidenteve sipas formatit dhe afateve të përcaktuara në këtë ligj dhe në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit;

dh) ruan log-e për një periudhë të përcaktuar në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit;

e) mban dhe ruan kronologjinë e të gjitha provave të incidentit në përputhje me dispozitat e këtij ligji dhe legjislacionin në fuqi për mbrojtjen e të dhënave personale;

ë) raporton pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial çdo incident të sigurisë kibernetike të ndodhur në infrastrukturat e tyre;

f) zbaton politikat e sigurisë kibernetike në nivel institucional.

Neni 18
Pikat e kontaktit

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit caktojnë pikat e kontaktit sipas përcaktimeve të bëra në këtë ligj.

2. Në të dhënat për pikat e kontaktit për personat juridikë publikë dhe privatë përfshihen:

a) emri;

b) adresa e selisë;

c) numri i identifikimit (NUIS) të personit juridik ose numri i ngjashëm, i caktuar jashtë vendit;

ç) të dhënat e personit të kontaktit që është i autorizuar të veprojë në emër të operatorit, përfshirë adresën e *e-mail*-it, rangjet IP dhe numrat e telefonit.

3. Pikat e kontaktit raportohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial brenda 15 ditëve pas hyrjes në fuqi të listës së infrastrukturave kritike dhe të rëndësishme të informacionit, të miratuar me vendim të Këshillit të Ministrave.

4. Çdo ndryshim në të dhënat e pikave të kontaktit i komunikohet zyrtarisht CSIRT-it Kombëtar dhe CSIRT-it sektorial nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit brenda 7 ditëve kalendarike.

Neni 19
Shkëmbimi i informacionit

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit shkëmbejnë vullnetarisht ndërmjet tyre informacione në lidhje me kërcënimet kibernetike, vulnerabilitetet, treguesit e kompromisit, teknikat dhe procedurat, informacione specifike për aktorët e kërcënimit, sinjalizime dhe rekomandime për sigurinë kibernetike, konfigurimin e mjeteve të sigurisë kibernetike për zbulimin e sulmeve kibernetike, me qëllim:

a) parandalimin, zbulimin, reagimin ndaj incidenteve kibernetike ose rikuperimin apo zvogëlimin e ndikimit të incidenteve kibernetike;

b) rritjen e nivelit të sigurisë kibernetike, veçanërisht nëpërmjet rritjes së ndërgjegjësimit në lidhje me kërcënimet kibernetike, duke kufizuar ose penguar përhapjen e kërcënimeve të tilla, duke u mbështetur në një sërë kapacitetesh mbrojtëse, korrigjimin dhe zbulimin e vulnerabiliteteve, teknikat e zbulimit, kontrollit dhe parandalimit të incidentit, reagimin dhe fazat e rikuperimit, si dhe promovimin e bashkëpunimit ndërmjet subjekteve publike dhe private referuar analizës së incidenteve kibernetike.

2. Shkëmbimi vullnetar i informacionit ndërmjet operatorëve bëhet nëpërmjet marrëveshjeve për shkëmbimin e informacionit të sigurisë kibernetike, duke ruajtur në çdo rast konfidencialitetin e informacionit.

3. Operatorët e infrastrukturave të informacionit, në përputhje me përcaktimet e këtij neni, kanë detyrimin të njoftojnë Autoritetin në çdo rast lidhur me nënshkrimin dhe përfundimin e marrëveshjeve për ndarjen e informacionit.

KREU III
ADMINISTRIMI I SIGURISË KIBERNETIKE

Neni 20
Masat e sigurisë kibernetike

1. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit janë të detyruar të zbatojnë masat e sigurisë, si dhe të dokumentojnë zbatimin e tyre sipas përcaktimeve të bëra në këtë ligj.

2. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit, me qëllim garantimin e vazhdimësisë së shërbimeve, implementojnë masa të përshtatshme dhe proporcionale për të arritur një nivel të lartë të sigurisë kibernetike në infrastrukturat e tyre.

3. Masat e sigurisë kibernetike klasifikohen në masa organizative, masa teknike dhe masa operacionale për menaxhimin e riskut dhe përditësohen nga Autoriteti duke marrë në konsideratë zhvillimet e fundit teknologjike.

4. Masat e sigurisë kibernetike kanë për qëllim parandalimin dhe minimizimin e efektit të incidentit në sigurinë e rrjeteve dhe të sistemeve të informacionit.

5. Përmbajtja dhe mënyra e dokumentimit të masave organizative, teknike dhe operacionale të sigurisë kibernetike përcaktohen me vendim të Këshillit të Ministrave.

6. Subjektet, të cilat operojnë në sektorët sipas anekseve të këtij ligji, por që nuk janë ende pjesë e listës së infrastrukturave të informacionit, mund të aplikojnë apriori të gjitha masat e sigurisë kibernetike sipas përcaktimeve të bëra në këtë ligj.

Neni 21

Masat për menaxhimin e riskut për operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit

1. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit zbatojnë masa teknike, organizative dhe operacionale për menaxhimin e riskut, të cilat përfshijnë:

a) përcaktimin e politikave për analizën e riskut të incidentit dhe sigurinë e sistemit të informacionit;

b) trajtimin e incidentit;

c) vazhdimësinë e punës, si menaxhimi i *backup*-it dhe rikuperimit, rimëkëmbjen nga katastrofat dhe menaxhimin e krizave;

ç) sigurinë e zinxhirit të furnizimit, duke përfshirë aspektet e lidhura me sigurinë në lidhje me marrëdhëniet midis çdo njësie dhe furnizuesit të drejtpërdrejtë të tij ose ofruesit e shërbimeve;

d) sigurinë në blerjen, zhvillimin dhe mirëmbajtjen e sistemeve të informacionit dhe rrjetit, duke përfshirë trajtimin dhe zbulimin e vulnerabiliteteve;

dh) politikat dhe procedurat për të vlerësuar efektivitetin e masave të menaxhimit të riskut të sigurisë kibernetike;

e) praktikat bazë të higjienës kibernetike dhe trajnimet për sigurinë kibernetike;

ë) politikat dhe procedurat në lidhje me përdorimin e kriptografisë dhe, sipas rastit, enkriptimin;

f) sigurinë e burimeve njerëzore, politikat e kontrollit të aksesit dhe menaxhimin e aseteve;

g) përdorimin e autentifikimit me shumë faktorë ose zgjidhjeve të vërtetimit të vazhdueshëm, zëri i siguruar, video dhe teksti, komunikimet dhe sistemet e sigurta të komunikimit të emergjencës brenda njësisë, sipas rastit.

2. Gjatë zbatimit të masave organizative, teknike dhe operacionale për menaxhimin e riskut operatorët marrin në konsideratë veçanërisht:

a) sigurinë e rrjeteve dhe sistemeve të shërbimeve;

b) menaxhimin e incidentit;

c) menaxhimin e vazhdimësisë së shërbimit dhe të rimëkëmbjes nga katastrofat;

ç) monitorimin, auditimin dhe testimin;

d) përputhshmërinë me standardet ndërkombëtare.

Neni 22

Masat e sigurisë kibernetike në rast kërcënimi ose incidenti të sigurisë kibernetike

1. Në rast të një incidenti kibernetik apo kërcënimi të mundshëm, aplikohen masat e sigurisë kibernetike të kategorizuara si më poshtë:

a) masa paralajmëruese;

b) kundërmasat dhe *playbooks*;

c) masa mbrojtëse të natyrës së përgjithshme.

2. Masat paralajmëruese janë masa me karakter rekomandues, që jepen nga Autoriteti në rastet e një kërcënimi të ndodhur dhe vendosen në dispozicion të operatorëve për t'u implementuar menjëherë. Masat paralajmëruese hartohen nga Autoriteti dhe miratohen me urdhër të drejtorit të përgjithshëm të Autoritetit.

3. Kundërmasat hartohen nga Autoriteti dhe ndërmerren nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit për incidentin e ndodhur në infrastrukturat e tyre. Autoriteti harton *playbooks* bazuar në kategoritë e incidenteve të sigurisë kibernetike të ENISA-s, të cilët aplikohen sipas rastit të incidentit të sigurisë kibernetike të paraqitur. Personi përgjegjës, në cilësinë e pikës së kontaktit, informon menjëherë Autoritetin për zbatimin e kundërmasave, *playbooks* dhe rezultatin e tyre. Miratimi dhe zbatimi i kundërmasave dhe *playbooks* bëhet me urdhër të drejtorit të përgjithshëm të Autoritetit.

4. Masat mbrojtëse të natyrës së përgjithshme janë masat e bazuara në një analizë të incidenteve të sigurisë kibernetike, tashmë të zgjidhura, me qëllim rritjen e mbrojtjes së rrjeteve dhe sistemeve të informacionit dhe zbatohen nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit. Masat mbrojtëse të natyrës së përgjithshme përcaktohen në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit.

Neni 23

Rreziqet e sigurisë kibernetike dhe raportimi i incidenteve të sigurisë kibernetike

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit marrin masa për të parandaluar e minimizuar ndikimin e rreziqeve dhe të incidenteve të sigurisë kibernetike në infrastrukturat e tyre të informacionit.

2. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit bashkëpunojnë me CSIRT-in Kombëtar dhe CSIRT-in sektorial në të gjitha fazat e një incidenti kibernetik të ndodhur në infrastrukturat e tyre të informacionit.

3. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit raportojnë të gjitha llojet e incidenteve të sigurisë kibernetike pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial, brenda 4 orëve nga momenti i identifikimit të incidentit. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në rastin e incidenteve të rëndësishme, brenda 72 orëve nga momenti i identifikimit të incidentit të rëndësishëm përditësojnë informacionin dhe bëjnë një vlerësim fillestar të incidentit të rëndësishëm, duke përfshirë ashpërsinë dhe ndikimin, si dhe, aty ku ka, treguesit e kompromitimit.

4. Për të përcaktuar rëndësinë e ndikimit të një incidenti kibernetik vlerësohen parametrat e mëposhtëm:

a) numri i përdoruesve të prekur nga ndërprerja e shërbimit;

b) kohëzgjatja e incidentit;

c) shtrirja gjeografike në lidhje me zonën e prekur nga incidenti;

ç) shkalla e ndërprerjes së funksionimit të shërbimit;

d) shtrirja e ndikimit në aktivitetet ekonomike dhe shoqërore;

dh) varësia e sektorëve nga shërbimet e ofruara të operatorit të infrastrukturës së informacionit;

e) rëndësia e ruajtjes së një niveli të mjaftueshëm të shërbimit, duke marrë parasysh disponueshmërinë e mjeteve alternative për sigurimin e këtij shërbimi.

5. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, brenda një muaji pas njoftimit të incidentit, sipas pikës 3 të këtij neni, i dorëzojnë CSIRT-it Kombëtar një raport përfundimtar, i cili përmban:

a) një përshkrim të detajuar të incidentit, duke përfshirë rëndësinë dhe ndikimin e tij;

b) llojin e kërcënimit ose shkakun kryesor që mund ta ketë shkaktuar incidentin;

c) masat e zbatuara dhe masat e vazhdueshme për zvogëlimin e pasojave;

ç) aty ku është e aplikueshme, ndikimin ndërkufitar të incidentit.

6. Në rastet e një incidenti kibernetik të vazhdueshëm, operatori i infrastrukturës së informacionit i prekur nga ky incident, përveç detyrimit të dorëzimit të raportit përfundimtar sipas pikës 5 të këtij neni, ka detyrimin të dorëzojë pranë CSIRT-it Kombëtar edhe një raport progresi në kohën e ndodhjes së incidentit kibernetik.

7. Autoriteti vendos në dispozicion të organizmave ndërkombëtarë në fushën e sigurisë kibernetike të dhënat e administruara në lidhje me incidentet e sigurisë kibernetike, me qëllim trajtimin dhe zgjidhjen e tyre. Komunikimi dhe ndarja e të dhënave sipas përcaktimeve të kësaj pike bëhet në përputhje me legjislacionin në fuqi për marrëveshjet ndërkombëtare dhe për mbrojtjen e të dhënave personale.

8. Llojet dhe kategoritë e incidenteve të sigurisë kibernetike, të cilat prekin sistemet dhe rrjetet e informacionit, formatin, elementet e raportimit, afatet e raportimit, mënyrën e dokumentimit dhe të regjistrimit të incidenteve kibernetike përcaktohen me rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit.

Neni 24

Masat shtesë të sigurisë kibernetike

Operatorët e infrastrukturave kritike të informacionit, përveç masave të sigurisë kibernetike të parashikuara në nenet 21 dhe 22 të këtij ligji, mund të miratojnë masa shtesë të menaxhimit të riskut apo të njoftimit të incidenteve të sigurisë kibernetike, të cilat janë në përputhje me aktet rregullatore të Bashkimit Evropian dhe që nuk bien në kundërshtim me përcaktimet e bëra në këtë ligj.

Neni 25

Njoftimi vullnetar i incidenteve të sigurisë kibernetike

1. Përveç operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit raportojnë vullnetarisht edhe subjekte të tjera.

2. CSIRT-i Kombëtar shqyrton raportimet e bëra dhe, në varësi të tyre, përcakton rëndësinë e ndikimit të incidentit kibernetik, sipas parametrave të përmendur në pikën 4 të nenit 23 të këtij ligji, duke zbatuar në çdo rast parimin e konfidencialitetit.

3. Raportimet vullnetare shqyrtohen nga Autoriteti vetëm pasi është vlerësuar që këto raportime nuk ndikojnë në trajtimin e raportimeve të detyrueshme të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit.

4. Raportimi vullnetar nuk krijon pasoja apo detyrime për subjektin raportues, nëse ai nuk do të kishte bërë një raportim të tillë.

Neni 26

Informimi i publikut dhe i përdoruesve për incidentet kibernetike

1. CSIRT-i Kombëtar, pasi është konsultuar me operatorin e infrastrukturës së informacionit, informon publikun për incidentet e ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit, kur ky informim është i nevojshëm për ndërgjegjësimin e publikut, për të parandaluar një incident të rëndësishëm, trajtimin e incidentit apo kur prek interesin publik, ose i kërkon operatorit të infrastrukturës së informacionit ta bëjë këtë duke ruajtur konfidencialitetin e të dhënave të incidentit.

2. Informimi i publikut bëhet sipas një procedure komunikimi të miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit.

3. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit njoftojnë pa vonesë përdoruesit e shërbimeve të tyre, të cilët janë prekur potencialisht nga një incident kibernetik i rëndësishëm, në lidhje me masat që këta përdorues janë në gjendje të marrin si përgjigje ndaj atij kërcënimi.

4. Një incident kibernetik konsiderohet i rëndësishëm, nëse:

a) ka shkaktuar ose është në gjendje të shkaktojë ndërprerje të rëndë operacionale të shërbimeve ose humbje financiare për operatorin e prekur;

b) ka ndikuar ose është në gjendje të prekë persona të tjerë fizikë ose juridikë, duke shkaktuar dëme të konsiderueshme materiale ose jomateriale.

5. Nëse një incident kibernetik i raportuar prek një ose më shumë shtete të tjera, CSIRT-i Kombëtar informon shtetet e prekura në përputhje me dispozitat e këtij ligji dhe legjislacionin në fuqi për mbrojtjen e të dhënave personale.

Neni 27

Kufizimi i të dhënave dhe ruajtja e konfidencialitetit

1. Nëpunësit e Autoritetit, që marrin pjesë në zgjidhjen e incidentit kibernetik, janë të detyruar të ruajnë konfidencialitetin e plotë për të gjitha të dhënat e përpunuara gjatë procedurës së zgjidhjes së tij.

2. Konfidencialiteti i të dhënave ruhet edhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin në përputhje me parashikimet ligjore në fuqi.

3. Konfidencialiteti i të dhënave të incidentit kibernetik trajtohet sipas legjislacionit në fuqi për informacionin e klasifikuar dhe legjislacionin në fuqi për mbrojtjen e të dhënave personale.

Neni 28

Kriza kibernetike

1. Në rastet kur nga subjektet përgjegjëse të sigurisë kibernetike është e pamundur të shmanget një kërcënim kibernetik drejt rrjeteve dhe sistemeve të informacionit, Autoriteti, në koordinim me subjektet e tjera përgjegjëse të sigurisë dhe mbrojtjes, sipas shkronjës "a" të nenit 11 të këtij ligji, i propozon menjëherë Kryeministrit shpalljen e gjendjes së krizës kibernetike dhe masat emergjente për zgjidhjen e situatës.

2. Gjendja e krizës kibernetike shpallet me vendim të Këshillit të Ministrave, me propozimin e Kryeministrit. Vendimi për shpalljen e gjendjes së krizës kibernetike njoftohet në media.

3. Gjendja e krizës kibernetike shpallet për një periudhë kohore deri në 7 ditë. Kjo periudhë mund të zgjatet në mënyrë të përsëritur, në varësi të kompleksitetit të situatës kibernetike, me vendim të Këshillit të Ministrave. Periudha maksimale e shpalljes së gjendjes së krizës kibernetike nuk duhet të kalojë 30 ditë.

4. Gjatë periudhës së gjendjes së krizës kibernetike, drejtori i përgjithshëm i Autoritetit informon Kryeministrin në lidhje me ecurinë dhe zgjidhjen e kësaj gjendjeje, si dhe për kërcënimet reale të mundshme.

5. Gjatë gjendjes së krizës kibernetike, Autoriteti koordinon menaxhimin e krizës dhe ka të drejtë të nxjerrë vendime me karakter të përgjithshëm ose të marrë masa mbrojtëse të natyrës së përgjithshme dhe kundërmasa.

6. Kundërmasat e nxjerra nga Autoriteti para vendosjes së gjendjes së krizës kibernetike mbeten në fuqi për aq kohë sa këto kundërmasa nuk bien në kundërshtim me masat emergjente të deklaruara nga Këshilli i Ministrave.

7. Autoriteti koordinon veprimet e të gjitha strukturave përgjegjëse për zgjidhjen e gjendjes së krizës kibernetike.

8. Në përputhje me përcaktimet e bëra sa më sipër, Autoriteti miraton një plan kombëtar për reagimin ndaj incidenteve të sigurisë kibernetike në shkallë të gjerë dhe ndaj krizës kibernetike, i cili përcakton:

a) objektivat dhe masat e përgatitjes në nivel kombëtar, si dhe aktivitetet;

b) detyrat dhe përgjegjësitë e subjekteve përgjegjëse për menaxhimin e krizës kibernetike;

c) procedurat e menaxhimit të kizës kibernetike, duke përfshirë integrimin e tyre në kuadrin ligjor kombëtar të menaxhimit të përgjithshëm të krizës kibernetike, si dhe kanalet e shkëmbimit të informacionit;

ç) masat kombëtare të përgatitjes, duke përfshirë ushtrimet dhe aktivitetet e trajnimit;

d) palët përkatëse publike dhe private, si dhe infrastrukturat e përfshira;

dh) procedurat dhe marrëveshjet kombëtare ndërmjet Autoritetit dhe organeve përkatëse kombëtare për të siguruar pjesëmarrjen efektive dhe mbështetjen në menaxhimin e koordinuar të incidenteve të sigurisë kibernetike dhe krizave kibernetike në shkallë të gjerë në nivel kombëtar.

9. Procedurat për identifikimin, klasifikimin, përshkallëzimin dhe menaxhimin e krizës kibernetike përcaktohen me vendim të Këshillit të Ministrave.

Neni 29

Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike – CERT

1. Me qëllim trajtimin në kohë dhe me eficiencë të emergjencave dhe të krizës së sigurisë kibernetike, në përputhje me përcaktimet e këtij ligji, krijohet pranë Autoritetit një strukturë *ad-hoc*, rast pas rasti, i quajtur Ekipi i Përgjigjes ndaj Emergjencave të Sigurisë Kibernetike – CERT.

2. CERT-i përbëhet nga ekspertë të fushës, të cilët thirren nga Autoriteti për hartimin e planit të masave të emergjencës, menaxhimin dhe zgjidhjen e emergjencave dhe krizës kibernetike.

3. CERT-i, gjatë ushtrimit të detyrave të tij, ka detyrimin e respektimit të parimit të konfidencialitetit.

4. Ngritja, mënyra e organizimit dhe funksionimit të CERT-it përcaktohen me vendim të Këshillit të Ministrave.

KREU IV
MBIKËQYRJA DHE ZBATIMI I MASAVE TË SIGURISË KIBERNETIKE

Neni 30
Mbikëqyrja dhe zbatimi i masave të sigurisë kibernetike

1. Autoriteti kontrollon zbatimin e masave të sigurisë kibernetike nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

2. Autoriteti, në funksion të ushtrimit të veprimtarisë mbikëqyrëse, ushtron këto kompetenca:

a) mbikëqyr operatorët nëpërmjet kontrolleve periodike, si dhe sa herë e gjykon të arsyeshme, në çdo rast, duke njoftuar operatorin 10 ditë pune përpara kryerjes së kontrollit;

b) zhvillon kontrolle për rrjetet dhe sistemet e deklaruara, si dhe çdo rrjet apo sistem tjetër apo të ndërlidhur me to nëpërmjet një plani vjetor kontrolli të hartuar në fillim të çdo viti, i cili miratohet me urdhër të drejtorit të përgjithshëm të Autoritetit, si dhe publikohet në faqen zyrtare të Autoritetit;

c) zhvillon kontrolle me grupe *ad-hoc* në rastet e një incidenti kibernetik të ndodhur ose në rastet e shkeljeve të mundshme të këtij ligji;

ç) zhvillon skanime të jashtme të rrjeteve dhe sistemeve të operatorëve, për efekt të kontrollit të masave të sigurisë në lidhje me vulnerabilitete të mundshme, në çdo rast, duke informuar paraprakisht operatorin e infrastrukturës së informacionit, duke siguruar transparencë të procesit dhe garantuar konfidencialitetin e informacionit;

d) kërkon informacionin e nevojshëm për vlerësimin e nivelit të sigurisë së rrjeteve dhe sistemeve të informacionit për të aksesuar masat e menaxhimit të riskut të ndërmarra nga operatorët;

dh) mbledh të dhëna, dokumente dhe informacionin e nevojshëm për të kryer funksionin e tij mbikëqyrës ndaj operatorëve, duke informuar paraprakisht operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit dhe garanton mbrojtjen e këtij informacioni;

e) kërkon dhe verifikon evidencat e dokumentuara për zbatimin efektiv të politikave të sigurisë kibernetike në kuadër të procesit të kontrollit.

Neni 31
Detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë të gjitha infrastrukturat e tyre kritike, të rëndësishme, si dhe të gjitha infrastrukturat e tjera që ndërveprojnë me to pranë Autoritetit.

2. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë pranë Autoritetit në vazhdimësi çdo infrastrukturë të re, të administruar prej tyre, që ndërvepron me infrastrukturat e kategorizuara kritike apo të rëndësishme.

3. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të dokumentojnë çdo ndryshim dhe zhvillim të kryer në infrastrukturat e tyre kritike dhe të rëndësishme.

4. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të vendosin në dispozicion të Autoritetit çdo dokumentacion dhe evidencë që kërkohet nga Autoriteti në kuadër të procesit të kontrollit.

5. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në kuadër të aktivitetit mbikëqyrës, i ofrojnë CSIRT-it Kombëtar akses të drejtpërdrejtë në ambientet dhe sistemet e tyre të

informacionit, në zbatim të procedurave të sigurisë të çdo operatori të këtyre infrastrukturave, të cilat janë të lidhura me shërbimet e ofruara prej tyre.

6. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të zbatojnë masat korrigjuese të lëna nga Autoriteti, si dhe të raportojnë për zbatimin e tyre.

7. Për implementimin efektiv të masave të sigurisë kibernetike, operatorët paraqesin pranë Autoritetit raportin e vlerësimit të konformitetit nga një organ i vlerësimit të konformitetit për sigurinë kibernetike të paktën një herë në 2 vjet.

8. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të marrin masa të shtuara teknike, në përputhje me përcaktimet e bëra në vendimin e Këshillit të Ministrave, për përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë kibernetike.

9. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të bashkëpunojnë me Autoritetin në kuadër të realizimit të funksioneve mbikëqyrëse, të përcaktuara në këtë ligj.

Neni 32

Detyrime të tjera të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publike

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publike, sipas aneksit 1 të këtij ligji, me qëllim garantimin e vendosjes së standardeve të sigurisë dhe ndërveprueshmërisë me sistemet qeveritare, përpara inicimit të implementimit të një sistemi, duhet të marrin konfirmimin e institucionit përgjegjës, sipas legjislacionit në fuqi për qeverisjen elektronike lidhur me specifikimet teknike.

2. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publike, sipas aneksit 1 të këtij ligji, hostojnë nyjën primare të infrastrukturës së tyre pranë Qendrës së të Dhënave Qeveritare dhe nyjën sekondare pranë Qendrës së Vazhdueshmërisë së Punës *(Business Continuity Center).*

3. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publike, sipas aneksit 1 të këtij ligji, monitorohen nga Qendra Kombëtare Operacionale e Sigurisë Kibernetike.

KREU V

BASHKËPUNIMI NË NIVEL KOMBËTAR DHE NDËRKOMBËTAR

Neni 33

Bashkëpunimi në nivel kombëtar

1. Autoriteti koordinon veprimtarinë e tij me institucionet e sigurisë dhe të mbrojtjes, si dhe bashkëpunon me subjektet e tjera përgjegjëse për sigurinë kibernetike sipas përcaktimeve të bëra në këtë ligj.

2. CSIRT-et pranë operatorëve, CSIRT-et sektoriale kanë detyrimin për të bashkëpunuar në çdo kohë me CSIRT-in Kombëtar dhe Autoritetin, në përmbushje të detyrimeve dhe përgjegjësive që rrjedhin nga ky ligj.

3. Në përputhje me pikën 1 të këtij neni, Autoriteti:

a) bashkëpunon me Policinë e Shtetit dhe institucionet përkatëse në rastet kur nga informacioni i siguruar për efekt të këtij ligji dyshon për elemente të krimit kibernetik ose veprave të tjera penale të lidhura me to;

b) bashkëpunon me institucionin përgjegjës për sigurinë e informacionit të klasifikuar në rastet kur merr dijeni për kërcënime të mundshme në rrjetet e klasifikuara, të infrastrukturave të informacionit, objekt i këtij ligji;

c) bashkëpunon me institucionin përgjegjës për komunikimet elektronike dhe postare, AKEP-in, për sigurinë e rrjeteve dhe shërbimeve të komunikimeve elektronike, si dhe për mbylljen e faqeve me përmbajtje të paligjshme dhe IP-eve, që gjenerojnë sulme, *malware*;

ç) bashkëpunon me Autoritetin Kombëtar për Mbrojtjen e të Dhënave Personale në rastet kur trajtohen incidente në infrastrukturat e informacionit, të cilat rezultojnë në përhapje të paligjshme të të dhënave personale.

Neni 34
Bashkëpunimi ndërkombëtar

1. Autoriteti bashkëpunon me organizmat ndërkombëtarë në fushën e sigurisë kibernetike dhe autoritetet kombëtare të vendeve të tjera nëpërmjet marrëveshjeve të përbashkëta në përputhje me legjislacionin në fuqi për marrëveshjet ndërkombëtare.

2. Në kuadër të përmbushjes së angazhimeve, në terma të sigurisë kibernetike, si vend anëtar i Aleancës Euro-Atlantike (NATO) dhe Organizatës për Sigurimin dhe Bashkëpunimin në Evropë (OSBE), Autoriteti koordinon dhe bashkërendon punën midis këtyre organizmave dhe institucioneve kombëtare.

3. Autoriteti bashkëpunon me grupin e bashkëpunimit, rrjetin e CSIRT-eve, rrjetin evropian të organizatave ndërlidhëse të krizave kibernetike (EU-CyCLONe), sipas përcaktimeve të bëra në këtë ligj.

4. Autoriteti merr pjesë në forumet ndërkombëtare për çështje të sigurisë kibernetike dhe bashkëpunon me to për rritjen e sigurisë kibernetike në vend.

Neni 35
Grupi i bashkëpunimit

Autoriteti merr pjesë në aktivitetet e grupit të bashkëpunimit, të përbërë nga përfaqësues të shteteve anëtare të Bashkimit Evropian, të Komisionit Evropian dhe të Agjencisë së Bashkimit Evropian për Rrjetin dhe Sigurinë e Informacionit (ENISA), duke kontribuuar kryesisht, për:

a) shkëmbimin e informacionit dhe të praktikave më të mira lidhur me:

i. kërcënimet kibernetike dhe incidentet e sigurisë kibernetike;

ii. vulnerabilitetet;

iii. trajnimet dhe rritjen e kapaciteteve;

iv. ndërgjegjësimin në fushën e sigurisë kibernetike;

v. standardet dhe specifikimet teknike;

vi. identifikimin e operatorëve kritikë dhe të rëndësishëm të informacionit;

vii. iniciativat e reja të politikave të sigurisë kibernetike dhe kërkesave të sektorëve specifikë për sigurinë kibernetike;

viii. zbatimin e akteve ligjore të Bashkimit Evropian të sektorëve specifikë, që përmbajnë dispozita për sigurinë kibernetike.

b) vlerësimin e procesit të rrezikut të zinxhirit të furnizimit në nivelin e BE-së lidhur me shërbimet TIK, sistemet TIK dhe produktet TIK;

c) rastet e ndihmës reciproke, duke përfshirë përvojat, rezultatet dhe veprimet e përbashkëta ndërkufitare;

ç) politikat për veprimet vijuese pas incidenteve dhe krizave të sigurisë kibernetike në shkallë të gjerë mbi bazën e mësimeve të nxjerra nga rrjeti i CSIRT-eve dhe EU-CyCLONE;

d) rishikimin e nivelit të sigurisë kibernetike, sipas përcaktimeve të bëra në nenin 38 të këtij ligji.

Neni 36
Rrjeti i CSIRT-eve

CSIRT-i Kombëtar merr pjesë në rrjetin e CSIRT-eve, duke kontribuuar kryesisht për:

a) shkëmbimin e informacionit dhe praktikave më të mira për kapacitetet e CSIRT-eve;

b) incidenteve të sigurisë kibernetike, kërcënimeve kibernetike, rreziqeve dhe vulnerabiliteteve;

c) dhënien e ndihmës në trajtimin e incidenteve ndërkufitare;

ç) format e bashkëpunimit operacional, duke përfshirë:

i. kategoritë e kërcënimeve dhe incidenteve kibernetike;

ii. paralajmërimet;

iii. ndihmën reciproke;

iv. parimet dhe marrëveshjet për koordinimin në përgjigje të rreziqeve dhe incidenteve ndërkufitare;

v. kontributin në incidentin kombëtar të sigurisë kibernetike në shkallë të gjerë dhe planin e reagimit ndaj krizave kibernetike, me kërkesë të një shteti anëtar.

d) bashkëpunimin dhe shkëmbimin e informacionit me qendrat operacionale të sigurisë (SOC), në nivel kombëtar dhe në nivel të Bashkimit Evropian, për ndërgjegjësimin e përbashkët të situatës për incidentet dhe kërcënimet e sigurisë kibernetike.

Neni 37

Rrjeti Evropian i Organizatave Ndërlidhëse të Krizave Kibernetike (EU-CyCLONe)

Autoriteti merr pjesë me Rrjetin Evropian të Organizatave Ndërlidhëse të Krizave Kibernetike (EU-CyCLONe), në kuadër të menaxhimit të incidenteve dhe krizave të sigurisë kibernetike në shkallë të gjerë, duke kontribuar kryesisht për:

a) rritjen e nivelit të gatishmërisë për menaxhimin e incidenteve dhe krizave të sigurisë kibernetike në shkallë të gjerë;

b) ndërgjegjësimin e përbashkët të situatës për incidentet dhe krizat e sigurisë kibernetike në shkallë të gjerë;

c) vlerësimin e pasojave dhe ndikimin e incidenteve dhe krizave të sigurisë kibernetike në shkallë të gjerë dhe propozimin e masave zbutëse;

ç) koordinimin e menaxhimit të incidenteve dhe krizave të sigurisë kibernetike në shkallë të gjerë;

d) ofron ndihmë, pas kërkesës së një shteti anëtar të interesuar, në rastet e incidenteve kombëtare të sigurisë kibernetike në shkallë të gjerë dhe planet e reagimit ndaj krizave të sigurisë kibernetike.

Neni 38

Rishikimi i sigurisë kibernetike në nivelin e Bashkimit Evropian

Autoriteti merr pjesë në rishikimin e nivelit të sigurisë kibernetike nëpërmjet ekspertëve të sigurisë kibernetike lidhur me:

a) nivelin e zbatimit të masave të menaxhimit të riskut të sigurisë kibernetike dhe detyrimeve, sipas përcaktimeve të bëra në këtë ligj;

b) nivelin e kapaciteteve, duke përfshirë burimet financiare, teknike dhe njerëzore në dispozicion dhe efektivitetin e ushtrimit të detyrave të autoriteteve kompetente;

c) kapacitetet operacionale të CSIRT-eve;

ç) nivelin e zbatimit të ndihmës reciproke, sipas përcaktimeve të bëra në këtë ligj;

d) nivelin e zbatimit të marrëveshjeve për ndarjen e informacionit të sigurisë kibernetike, sipas përcaktimeve të bëra në këtë ligj;

dh) çështje specifike të natyrës ndërkufitare ose ndërsektoriale.

KREU VI

CERTIFIKIMI I SIGURISË KIBERNETIKE

Neni 39

Përgatitja dhe rishikimi i një skeme kombëtare të certifikimit të sigurisë kibernetike

1. Autoriteti përgatit skemën kombëtare të certifikimit të sigurisë kibernetike në përputhje me skemat e miratuara të Bashkimit Evropian për certifikimin e sigurisë kibernetike.

2. Për përgatitjen e skemës kombëtare të certifikimit të sigurisë kibernetike, Autoriteti konsultohet me grupet e interesit nëpërmjet një procesi konsultimi formal, të hapur, transparent dhe gjithëpërfshirës.

3. Të paktën çdo pesë vjet, Autoriteti rishikon skemat e miratuara të certifikimit të sigurisë kibernetike, duke marrë në konsideratë sugjerimet e palëve të interesuara.

4. Autoriteti publikon në faqen e internetit në meny të dedikuar skemat kombëtare të certifikimit të sigurisë kibernetike, certifikatat e sigurisë kibernetike, si dhe informacion në lidhje me skemat që nuk janë më të vlefshme apo që janë shfuqizuar.

5. Një vit pas hyrjes në fuqi të skemës së certifikimit të sigurisë kibernetike, Autoriteti publikon listën e organeve të vlerësimit të konformitetit për sigurinë kibernetike të akredituar, sipas skemës së certifikimit të sigurisë kibernetike.

Neni 40

Objektivat e sigurisë së skemës kombëtare të certifikimit të sigurisë kibernetike

Një skemë kombëtare e certifikimit të sigurisë kibernetike përmbush, sipas rastit, të paktën objektivat e sigurisë si më poshtë:

a) mbrojtjen e të dhënave të ruajtura, të transmetuara ose të përpunuara, kundrejt zbulimit aksidental ose të paautorizuar, gjatë gjithë ciklit jetësor të produktit, shërbimit ose procesit TIK;

b) mbrojtjen e të dhënave të ruajtura, të transmetuara ose të përpunuara, ndaj shkatërrimit aksidental ose të paautorizuar, humbjes, ndryshimit apo mungesës së disponueshmërisë gjatë gjithë ciklit jetësor të produktit, shërbimit ose procesit TIK;

c) autorizimin e personave, programeve apo makinerive, vetëm për aksesin e të dhënave, shërbimeve ose funksioneve, të cilave u referohen të drejtat e tyre të aksesit;

ç) identifikimin dhe dokumentimin e vulnerabiliteteve të konstatuara;

d) regjistrimin e të dhënave, shërbimeve apo funksioneve, të cilat janë aksesuar, përdorur ose përpunuar, përfshirë kohën dhe individin;

dh) bërjen të mundur të kontrollit se cilat të dhëna, shërbime ose funksione janë aksesuar, përdorur ose përpunuar, përfshirë kohën dhe autorësinë;

e) verifikimin që produktet, shërbimet dhe proceset TIK nuk përmbajnë vulnerabilitete të njohura;

ë) rivendosjen e disponueshmërisë dhe të aksesit ndaj të dhënave, shërbimeve dhe funksioneve në kohën e duhur, në rast të një incidenti fizik ose teknik;

f) produktet, shërbimet dhe proceset TIK janë të sigurta që në projektim;

g) produktet, shërbimet dhe proceset TIK janë të pajisura me *software* dhe *hardware* të përditësuara, të cilat nuk përmbajnë vulnerabilitete të njohura dhe janë pajisur me mekanizma për përditësime të sigurta.

Neni 41

Certifikimi i produkteve, shërbimeve dhe proceseve të veçanta TIK

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit përdorin produkte, shërbime dhe procese TIK, të zhvilluara nga vetë operatorët ose të ofruara nga palë të treta, të certifikuara sipas skemës kombëtare të certifikimit të sigurisë kibernetike ose një skemë evropiane të certifikimit të sigurisë kibernetike.

2. Me qëllim rritjen e nivelit të sigurisë kibernetike në infrastrukturat e informacionit, Autoriteti inkurajon operatorët për përdorimin e identifikimit elektronik dhe shërbimeve të besuara të kualifikuara, sipas kuadrit ligjor në fuqi për to.

Neni 42

Miratimi i skemave, niveleve dhe organeve përgjegjëse për certifikimin e sigurisë kibernetike

1. Përcaktohen me vendim të Këshillit të Ministrave:

a) skema kombëtare e certifikimit të sigurisë kibernetike, e cila është në përputhje me skemat e certifikimit të miratuara nga Bashkimi Evropian, si dhe afatet lidhur me implementimin e skemës së certifikimit të sigurisë kibernetike nga subjektet e këtij ligji;

b) nivelet e sigurisë së skemës kombëtare të certifikimit të sigurisë kibernetike për produktet, shërbimet dhe proceset e TIK-ut.

2. Procedura dhe kriteret për regjistrimin e organeve të vlerësimit të konformitetit për sigurinë kibernetike, sipas skemës së certifikimit të sigurisë kibernetike, përcaktohen me udhëzimin e drejtorit të përgjithshëm të Autoritetit.

3. Këshilli i Ministrave miraton masën e tarifës së regjistrimit që organet e vlerësimit të konformitetit për sigurinë kibernetike duhet t'i paguajnë Autoritetit, në zbatim të detyrimeve të përcaktuara në këtë ligj.

4. Të ardhurat e përfituara nga tarifa e regjistrimit derdhen në buxhetin e shtetit.

KREU VII
MASAT ADMINISTRATIVE

Neni 43
Masat korrigjuese

1. Kur Autoriteti konstaton mangësi në zbatimin e masave të sigurisë, në zbatim të këtij ligji, përcakton një afat të arsyeshëm brenda të cilit operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit marrin masat korrigjuese përkatëse.

2. Kur Autoriteti konstaton se nga ana e operatorëve të infrastrukturave të informacionit nuk është zbatuar detyrimi i përcaktuar në pikën 2 të nenit 31 të këtij ligji, përcakton një afat të arsyeshëm brenda të cilit operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit marrin masat për përmbushjen e detyrimit.

3. Kostot lidhur me zbatimin e masave korrigjuese mbulohen nga operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit.

4. Operatorët janë të detyruar të njoftojnë Autoritetin për marrjen e masave korrigjuese, brenda afatit të përcaktuar, dhe të paraqesin dokumentacionin mbështetës për këto masa.

5. Kategorizimi i afateve, sipas llojit dhe mangësive të konstatuara, sipas përcaktimeve të bëra në pikat 1 dhe 2 të këtij neni, përcaktohet në vendimin e Këshillit të Ministrave për përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë kibernetike, sipas nenit 20 të këtij ligji.

Neni 44
Kundërvajtjet administrative

Në kuptim të këtij ligji, përbëjnë kundërvajtje administrative shkeljet e mëposhtme:

a) mosraportimi pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial të incidentit të sigurisë kibernetike të ndodhur në infrastruktura, sipas përcaktimit në shkronjën "ë" të pikës 3 të nenit 17 dhe pikës 3 të nenit 23 të këtij ligji;

b) mosraportimi i saktë i infrastrukturave të informacionit gjatë procesit të identifikimit, sipas përcaktimeve të pikës 4 të nenit 12 të këtij ligji dhe akteve nënligjore në zbatim të tij;

c) mosraportimi pranë Autoritetit të pikës së kontaktit apo i përditësimeve të tyre, sipas përcaktimeve në pikat 3 dhe 4 të nenit 18 të këtij ligji;

ç) mospërmbushja e detyrimeve të caktuara nga Autoriteti, në zbatim të pikës 1 të nenit 27 të këtij ligji;

d) mospërmbushja e detyrimeve nga ana e operatorëve, sipas përcaktimeve në pikat 1, 3, 4, 5, 7, 8 dhe 9 të nenit 31 të këtij ligji;

dh) mospërmbushja e detyrimeve nga ana e operatorëve, në zbatim të pikave 1, 2, 4 të nenit 43 të këtij ligji;

e) mospërmbushja e detyrimeve, të përcaktuara në pikat 5 dhe 6 të nenit 23 të këtij ligji;

ë) mospërmbushja e detyrimeve të përcaktuara në pikat 1 dhe 2 të nenit 32 të këtij ligji.

Neni 45
Sanksionet administrative

1. Kur Autoriteti konstaton shkeljen e dispozitave, të cilat përbëjnë kundërvajtje administrative, sipas nenit 44 të këtij ligji vendos dënimin me gjobë si më poshtë:

a) nga 1 000 000 deri në 10 000 000 lekë në rast të shkeljeve administrative të përcaktuara në shkronjat "a" dhe "d" të nenit 44 të këtij ligji;

b) nga 200 000 deri në 400 000 lekë në rast të shkeljeve administrative të përcaktuara në shkronjat "b", "c", "ç" dhe "e" të nenit 44 të këtij ligji;

c) nga 400 000 lekë deri në 1 000 000 lekë në rast të shkeljeve administrative të përcaktuara në shkronjën "dh" të nenit 44 të këtij ligji;

ç) nga 2 000 000 lekë deri në 5 000 000 lekë në rast të shkeljeve administrative të përcaktuara në shkronjën "ë" të nenit 44 të këtij ligji.

2. Metodologjia për përcaktimin e masës së dënimit administrativ gjobë përcaktohet me urdhër të drejtorit të përgjithshëm të Autoritetit.

3. Të ardhurat e siguruara nga kundërvajtjet administrative derdhen 100 për qind në buxhetin e shtetit.

Neni 46
Pezullimi i ushtrimit të shërbimit

1. Kur Autoriteti konstaton shkelje të përsëritura lidhur me zbatimin e masave të sigurisë kibernetike të përcaktuara në këtë ligj nga operatori i infrastrukturës kritike të informacionit, ndaj të cilit rezulton se janë marrë deri në 2 masa administrative të njëpasnjëshme, për mospërmbushjen e detyrimeve që rrjedhin nga ky ligj, njëkohësisht ka të drejtë:

a) t'i paraqesë kërkesë institucionit kompetent për bllokim të *domain*-it/nëndomeinit që lidhet me shërbimin;

b) t'i paraqesë kërkesë institucionit kompetent për licencimin, certifikimin apo autorizimin e shërbimit përkatës për pezullim të përkohshëm të licencës, autorizimit, lejes për ushtrimin e shërbimit për të cilin janë konstatuar mangësi të zbatimit të masave të sigurisë;

c) t'i paraqesë kërkesë institucionit kompetent për pezullim të përkohshëm të drejtuesit ekzekutiv ose përfaqësuesit ligjor që është përgjegjës për menaxhimin në infrastrukturat kritike.

2. Kur ndaj operatorit të infrastrukturës kritike janë marrë masat e përcaktuara në shkronjat "a" ose "b" ose "c" të pikës 1 të këtij neni, këto masa vazhdojnë të zbatohen derisa operatori të ndërmarrë veprimet e nevojshme për korrigjimin e mangësive apo plotësimin e kërkesave për të cilat janë vendosur këto masa.

3. Kur operatori ka ndërmarrë masat për plotësimin e mangësive apo kërkesave të konstatuara për të cilat janë dhënë masat e përcaktuara në shkronjat "a" ose "b" ose "c" të pikës 1 të këtij neni, Autoriteti i drejtohet me kërkesë institucionit kompetent për heqjen e tyre.

Neni 47
Procedura e vendosjes së dënimit administrativ gjobë

Procedurat e konstatimit, shqyrtimit, ankimit dhe ekzekutimit të kundërvajtjeve administrative janë ato të parashikuara në ligjin në fuqi për kundërvajtjet administrative.

KREU VIII
DISPOZITA TË FUNDIT

Neni 48
Aktet nënligjore

1. Ngarkohet Këshilli i Ministrave që brenda 6 muajve nga hyrja në fuqi e këtij ligji të miratojë aktet nënligjore në zbatim të neneve 7, pikat 7, 9, shkronja "ë", 12, pika 2 dhe 20, pika 5, të këtij ligji.

2. Ngarkohet Këshilli i Ministrave që brenda 9 muajve nga hyrja në fuqi e këtij ligji të miratojë Strategjinë Kombëtare për Sigurinë Kibernetike në zbatim të nenit 6, pikat 4 dhe 5, të këtij ligji.

3. Ngarkohet Këshilli i Ministrave që brenda 9 muajve nga hyrja në fuqi e këtij ligji të miratojë aktet nënligjore në zbatim të neneve 28, pika 9, dhe 29, pika 4, të këtij ligji.

4. Ngarkohet drejtori i përgjithshëm i Autoritetit që brenda 6 muajve nga hyrja në fuqi e këtij ligji të nxjerrë aktet nënligjore në zbatim të neneve 13, shkronja "f", 15, pika 4, 22, pika 4, 23, pika 8, dhe 45, pika 2, të këtij ligji.

5. Ngarkohet drejtori i përgjithshëm i Autoritetit që brenda 9 muajve nga hyrja në fuqi e këtij ligji, të nxjerrë aktin nënligjor në zbatim të shkronjës " k" të nenit 13 të këtij ligji.

6. Ngarkohet drejtori i përgjithshëm i Autoritetit që brenda 12 muajve nga hyrja në fuqi e këtij ligji të nxjerrë aktin nënligjor në zbatim të shkronjës "gj" të nenit 13 të këtij ligji.

7. Ngarkohet drejtori i përgjithshëm i Autoritetit që brenda 12 muajve nga hyrja në fuqi e këtij ligji të miratojë *playbooks* përkatëse në zbatim të pikës 3 të nenit 22 të këtij ligji.

8. Ngarkohet Këshilli i Ministrave që brenda 12 muajve nga hyrja në fuqi e këtij ligji të miratojë mënyrën e ngritjes së CSIRT-eve sektoriale në zbatim të pikës 5 të nenit 15 të këtij ligji.

9. Ngarkohet Këshilli i Ministrave që brenda 12 muajve nga miratimi i skemës evropiane të certifikimit të sigurisë kibernetike të miratojë aktet nënligjore të përcaktuara në shkronjat "a" dhe "b, të pikës 1 të nenit 42 të këtij ligji.

10. Ngarkohet Këshilli i Ministrave që brenda 6 muajve nga miratimi i skemës së certifikimit të sigurisë kibernetike të miratojë aktin nënligjor në zbatim të pikës 3 të nenit 42 të këtij ligji.

11. Ngarkohet drejtori i përgjithshëm i Autoritetit që brenda 6 muajve nga miratimi i skemës së certifikimit të sigurisë kibernetike të nxjerrë aktin nënligjor në zbatim të pikës 2 të nenit 42 këtij ligji.

Neni 49
Shfuqizime

1. Ligji nr. 2/2017 "Për sigurinë kibernetike" shfuqizohet.

2. Nenet 10 dhe 10/1 të ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", i ndryshuar, shfuqizohen.

3. Aktet nënligjore, të miratuara në zbatim të ligjit nr. 2/2017, "Për sigurinë kibernetike", mbeten në fuqi edhe pas hyrjes në fuqi të këtij ligji, kur nuk bien në kundërshtim me dispozitat e këtij ligji, deri në miratimin e akteve nënligjore në zbatim të këtij ligji.

Neni 50
Dispozitat kalimtare

1. Subjektet përgjegjëse në fushën e sigurisë kibernetike janë të detyruara të harmonizojnë veprimtarinë e tyre me parashikimet e këtij ligji brenda 24 muajve nga data e hyrjes në fuqi e këtij ligji.

2. Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike vazhdon të ushtrojë veprimtarinë e tij si institucioni përgjegjës në fushën e sigurisë kibernetike deri në riorganizimin e tij në përputhje me dispozitat e këtij ligji.

3. Autoriteti Kombëtar për Sigurinë Kibernetike, pas hyrjes në fuqi të këtij ligji, do të vazhdojë të ushtrojë edhe kompetencat e tij sipas përcaktimeve të bëra në ligjin nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", i ndryshuar, dhe në ligjin nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar, deri në momentin e hyrjes në fuqi të ligjit të ri për identifikimin elektronik dhe shërbimet e besuara.

4. Detyrimet e parashikuara për CSIRT-in Kombëtar, sipas këtij ligji, zbatohen edhe për raportimet në organizmat përgjegjës të BE-së, në rastin e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian.

5. Me hyrjen në fuqi të këtij ligji dhe çdo dy vjet pas hyrjes së tij në fuqi, Autoriteti, në cilësinë e pikës së vetme kombëtare të kontaktit, u dërgon Komisionit Evropian dhe ENISA-s informacionin e nevojshëm për zbatimin e këtij ligji, në veçanti në lidhje me identifikimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, në përputhje me kërkesat e ligjit për mbrojtjen e të dhënave personale, për transferimin ndërkombëtar.

6. Në rastin e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian, Autoriteti raporton pranë Komisionit Evropian dhe ENISA-s një herë në vit llojet e incidenteve të ndodhura në Republikën e Shqipërisë.

7. Me anëtarësimin në Bashkimin Evropian të Republikës së Shqipërisë, Autoriteti njofton Komisionin Evropian për çdo skemë të certifikimit të sigurisë kibernetike, për organet e vlerësimit të konformitetit për sigurinë kibernetike që janë akredituar, si dhe për çdo ndryshim të mëvonshëm.

Neni 51

Hyrja në fuqi

1. Ky ligj hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

2. Nenet 35, 36, 37 dhe 38, të këtij ligji hyjnë në fuqi me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian.

Miratuar në datën 21.3.2024.

Shpallur me dekretin nr. 149, datë 16.4.2024, të Presidentit të Republikës së Shqipërisë, Bajram Begaj.

ANEKSI I

SEKTORË ME KRITIKALITET TË LARTË

Sektori	Nënsektori	Lloji i subjektit
Energjia	**Elektriciteti**	- Ndërmarrjet e energjisë elektrike - Operatorët e sistemit të shpërndarjes - Operatorët e sistemit të transmetimit - Prodhuesit - Operatorët e emëruar të tregut të energjisë elektrike - Pjesëmarrësit e tregut, persona fizikë ose juridikë që blejnë, shesin ose prodhojnë energji elektrike - Operatorët e një pike rimbushjeje, që janë përgjegjës për menaxhimin dhe funksionimin e një pike rimbushjeje, e cila ofron një shërbim rimbushjeje për përdoruesit fundorë, duke përfshirë shërbimin në emër dhe për llogari të një ofruesi të shërbimit *mobile*
	Ngrohja dhe ftohja qendrore	- Operatorët e ngrohjes qendrore ose të ftohjes qendrore
	Nafta	-Operatorët e tubacioneve të transmetimit të naftës - Operatorë të objekteve të prodhimit, përpunimit dhe trajtimit të naftës, magazinimit dhe transmetimit - Subjektet qendrore aksionare
	Gazi	- Ndërmarrjet e furnizimit - Operatorët e sistemit të shpërndarjes - Operatorët e sistemit të transmetimit - Operatorët e sistemit të ruajtjes - Operatorët e sistemit të gazit natyror të lëngëzuar - Ndërmarrjet e gazit natyror - Operatorët e objekteve të përpunimit dhe trajtimit të gazit natyror
	Hidrogjeni	- Operatorët e prodhimit, ruajtjes dhe transmetimit të hidrogjenit
Transporti	**Ajror**	- Transportuesit ajrorë për arsye tregtare - Subjektet menaxhuese të aeroportit - Operatorët e kontrollit të menaxhimit të trafikut, që ofrojnë kontroll të trafikut ajror
	Hekurudhor	- Menaxherët e infrastrukturës - Ndërmarrjet hekurudhore, duke përfshirë operatorët e objekteve të shërbimit
	Detar	- Kompanitë e transportit ujor të udhëtarëve dhe mallrave në brendësi, detare dhe bregdetare, duke mos përfshirë anijet individuale të operuara nga këto kompani - Organet menaxhuese të porteve, duke përfshirë objektet e tyre portuale dhe

		subjektet që operojnë punimet dhe pajisjet e përfshira brenda porteve - Operatorët e shërbimeve të trafikut të anijeve (VTS)
	Rrugor	- Autoritetet rrugore përgjegjëse për kontrollin e menaxhimit të trafikut, duke përjashtuar entet publike për të cilat menaxhimi i trafikut ose funksionimi i sistemeve inteligjente të transportit është një pjesë jothelbësore e veprimtarisë së tyre të përgjithshme - Operatorët e sistemeve inteligjente të transportit
Bankar		- Institucionet e kreditimit
Infrastruktura e tregjeve financiare		- Operatorët e tregjeve financiare - Palët qendrore (operatorët e infrastrukturave të tregjeve financiare)
Shëndetësor		- Ofruesit e kujdesit shëndetësor - Laboratorët mjekësorë - Subjektet që kryejnë veprimtari kërkimore dhe zhvillimore të produkteve medicinale - Subjektet prodhuese të produkteve farmaceutike bazë dhe preparateve farmaceutike - Subjektet që prodhojnë pajisje mjekësore që konsiderohen si kritike gjatë një emergjence të shëndetit publik (lista e pajisjeve kritike të urgjencës së shëndetit publik)
Subjektet që ofrojnë shërbime ose hostojnë sisteme për përpunimin dhe transmetimin e informacionit të klasifikuar, që lidhen më sigurinë publike		- Policia e Shtetit - Subjektet që ofrojnë shërbime në sektorët për përpunimin dhe transmetimin e informacionit të klasifikuar që lidhen me sigurinë publike
Furnizimi me ujë të pijshëm		- Furnizuesit dhe shpërndarësit e ujit të destinuar për konsum njerëzor
Ujërat e zeza		- Ndërmarrjet që mbledhin, asgjësojnë ose trajtojnë ujërat e zeza urbane, ujërat e zeza shtëpiake ose mbeturinat industriale, duke përjashtuar ndërmarrjet për të cilat grumbullimi, asgjësimi ose trajtimi i ujërave të zeza urbane, ujërave të zeza shtëpiake ose ujërave të zeza industriale është një pjesë jothelbësore e veprimtarisë së tyre të përgjithshme
Infrastrukturat digjitale	**Shërbime elektronike dhe komunikimi**	- Ofruesit e pikës së shkëmbimit të internetit *(Internet Exchange Point)* - Ofruesit e shërbimeve DNS, duke përjashtuar operatorët e serverave të emrave rrënjë (root name servers) - Operatorët e regjistrave të emrave TLD - Ofruesit e shërbimeve kompjuterike në renë kompjuterike *(cloud computing)* - Ofruesit e shërbimeve të qendrës së të dhënave *(Data centre service providers)* - Ofruesit e rrjetit të shpërndarjes së përmbajtjes - Ofruesit e shërbimeve të besuara - Ofruesit e rrjeteve publike të komunikimeve elektronike - Ofruesit e shërbimeve të komunikimeve elektronike të disponueshme për publikun - Ofruesit e shërbimeve vizive të disponueshme për publikun
Menaxhimi i shërbimeve TIK (biznes me biznes)		- Ofruesit e shërbimeve të menaxhuara - Ofruesit e shërbimeve të sigurisë të menaxhuara - Ofruesit e shërbimeve TIK - Ofruesit e shërbimeve për zhvillim dhe mirëmbajtje të sistemeve
Administrata publike		- Subjektet e administratës publike në nivel qendror - Subjektet e administratës publike në nivel rajonal - Institucionet e pavarura
Hapësira		- Operatorët e infrastrukturës tokësore, në pronësi, menaxhim dhe operim nga subjekte publike/private, që mbështesin ofrimin e shërbimeve të bazuara në hapësirë, duke përjashtuar ofruesit e rrjeteve publike të komunikimeve elektronike
Sektori arsimor		- Subjektet që ofrojnë shërbime në sektorin arsimor.
Turizmi		- Subjektet që ofrojnë shërbime në sektorin e turizmit

SEKTORË TË TJERË KRITIKË

Sektori	Nënsektori	Lloji i subjektit
Postar dhe shërbimet e korrierit		- Subjektet që ofrojnë shërbime postare, duke përfshirë ofruesit e shërbimit të korrierit
Menaxhimi i mbetjeve		- Subjektet që kryejnë menaxhimin e mbetjeve
Prodhimi, përpunimi dhe shpërndarja e kimikateve		- Ndërmarrjet që kryejnë prodhimin e substancave dhe shpërndarjen e substancave ose të përzierjeve
Prodhimi, procesimi dhe shpërndarja e ushqimit		- Subjektet që ofrojnë shërbime që lidhen me ushqimin e shpërndarjen me shumicë, si dhe me prodhimin e përpunimin industrial ushqimor në shkallë të gjerë
Prodhimi	**Prodhimi i pajisjeve mjekësore dhe në pajisje mjekësore diagnostikuese *vitro***	- Subjektet që prodhojnë pajisje mjekësore, pajisje *in vitro* diagnostike mjekësore me përjashtim të subjekteve që prodhojnë pajisje mjekësore të përmendura në aneksin I, sektori "shëndetësor".
	Prodhim i produkteve kompjuterike, elektronike dhe optike	- Ndërmarrjet që kryejnë ndonjë nga aktivitetet ekonomike të referuara për prodhimin e produkteve kompjuterike, elektronike dhe optike
	Prodhimi i pajisjeve elektrike	- Ndërmarrjet që kryejnë ndonjë nga aktivitetet ekonomike të referuara për prodhimin e pajisjeve elektrike
	Prodhim makinerish dhe pajisjesh n.e.c.	- Ndërmarrjet që kryejnë ndonjë nga aktivitetet ekonomike të referuara në prodhimin e makinerive dhe të pajisjeve n.e.c.
	Prodhimi i automjeteve, rimorkiove dhe gjysmërimorkiove	- Ndërmarrjet që kryejnë ndonjë nga aktivitetet ekonomike të referuara në prodhimin e mjeteve motorike, rimorkiove dhe gjysmërimorkiove
	Prodhimi i pajisjeve të tjera të transportit	- Ndërmarrjet që kryejnë ndonjë nga aktivitetet ekonomike të referuara në prodhimin e pajisjeve të tjera të transportit
Ofruesit e shërbimeve digjitale		- Ofruesit e tregjeve në internet - Ofruesit e motorëve të kërkimit në internet - Ofruesit e platformave të shërbimeve të rrjeteve sociale

ANEKSI III
EFEKTET FINANCIARE PËR NJË AFAT 5-VJEÇAR

Nr.	Lloji i kostos	Viti i parë			Viti i dytë			Viti i tretë			Viti i katërt			Viti i pestë		
		AKCESK	**AKSHI**	**Inst. rajonal Inst. e Pav & Ligjzbatuese**	**AKCESK**	**AKSHI**	**Inst. rajonal Inst. e Pav & Ligjzbatuese**	**AKCESK**	**AKSHI**	**Inst. rajonal Inst. e Pav & Ligjzbatuese**	**AKCESK**	**AKSHI**	**Inst. rajonal Inst. e Pav & Ligjzbatuese**	**AKCESK**	**AKSHI**	**Inst. rajonal Inst. e Pav & Ligjzbatuese**
		40%	**30%**	**30%**	**40%**	**30%**	**30%**	**40%**	**30%**	**30%**	**40%**	**30%**	**30%**	**40%**	**30%**	**30%**
1	Kosto për infrastrukturën për sigurinë kibernetike (gjithë teknologjia, pajisjet *hardware, software*, licencat, sistemet etj.)	187,088,600	140,316,450	140,316,450	1,430,987,360	1,073,240,520	1,073,240,520	940,658,240	705,493,680	705,493,680	40,000,000	30,000,000	30,000,000	40,000,000	30,000,000	30,000,000
2	Kosto për ngritjen dhe implementimin e standardeve	245,164,560	183,873,420	183,873,420	143,098,736	107,324,052	107,324,052	94,065,824	70,549,368	70,549,368	4,000,000	3,000,000	3,000,000	4,000,000	3,000,000	3,000,000
3	Kostot për rritjen e kapaciteteve (trajnimet)	367,746,840	275,810,130	275,810,130	367,746,840	275,810,130	275,810,130	294,197,472	220,648,104	220,648,104	220,648,104	165,486,078	165,486,078	220,648,104	165,486,078	165,486,078
Totali për institucion		**800,000,000**	**600,000,000**	**600,000,000**	**1,941,832,936**	**1,456,374,702**	**1,456,374,702**	**1,328,921,536**	**996,691,152**	**996,691,152**	**264,648,104**	**198,486,078**	**198,486,078**	**264,648,104**	**198,486,078**	**198,486,078**