

VENDIM
Nr. 723, datë 3.12.2025

PËR NGRITJEN, MËNYRËN E ORGANIZIMIT DHE TË FUNKSIONIMIT TË EKIPIT TË PËRGJIGJES NDAJ EMERGJENCAVE DHE KRIZËS SË SIGURISË KIBERNETIKE

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 4, të nenit 29, të ligjit nr. 25/2024, “Për sigurinë kibernetike”, me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

I. NGRITJA E EKIPIT TË PËRGJIGJES NDAJ EMERGJENCAVE DHE KRIZËS SË SIGURISË KIBERNETIKE

1. Pranë Autoritetit Kombëtar për Sigurinë Kibernetike (në vijim, AKSK-ja) ngrihet dhe funksionon Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike (në vijim, CERT-i), i cili është një strukturë *ad hoc*, rast pas rasti, përgjegjëse për trajtimin në kohë dhe me eficiencë të emergjencave dhe të krizës së sigurisë kibernetike në Republikën e Shqipërisë.

2. CERT-i kryesohet nga Autoriteti Kombëtar për Sigurinë Kibernetike dhe përbëhet nga:

a) përfaqësues nga institucionet publike, si më poshtë vijon:

i. Ministria e Punëve të Brendshme;

ii. Ministria e Mbrojtjes;

iii. Ministria për Evropën dhe Punët e Jashtme;

iv. Autoriteti i Komunikimeve Elektronike dhe Postare;

v. Shërbimi Informativ i Shtetit;

vi. Agjencia Kombëtare e Shoqërisë së Informacionit;

vii. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale;

viii. Policia e Shtetit;

b) ekspertë të sigurisë kibernetike, të teknologjisë së informacionit dhe ekspertë OT (*operational technology*), thirrja e të cilëve do të bëhet sipas përcaktimeve të pikave 7–12 të këtij kreu.

3. Titullarët e institucioneve, sipas shkronjës “a”, të pikës 2, të këtij kreu, brenda 5 (pesë) ditëve nga hyrja në fuqi e këtij vendimi, dërgojnë pranë AKSK-së emrat e përfaqësuesve të institucioneve të tyre, si dhe përditësojnë emrat e listës, në raste ndryshimesh, brenda 5 (pesë) ditëve nga ndodhja e këtyre ndryshimeve.

4. AKSK-ja, me urdhër të drejtorit të përgjithshëm, bazuar në situatën e emergjencës e të krizës kibernetike, rast pas rasti, duke marrë në konsideratë kompleksitetin e situatës, natyrën e sulmit, si dhe numrin e infrastrukturave të prekura, vendos për numrin e ekspertëve, që do të përfshihen në ekipin e CERT-it dhe profilet e tyre.

5. Kriteret që duhet të plotësojnë ekspertët e sigurisë kibernetike të teknologjisë së informacionit dhe ekspertët OT, për të qenë pjesë e CERT-it, janë, si më poshtë vijon:

a) Kriteret të përgjithshme:

i. të kenë zotësi të plotë për të vepruar;

ii. të kenë diplomë të nivelit të gjashtë të Kornizës Shqiptare të Kualifikimeve, “Bachelor” ose të barasvlershme me të, sipas legjislacionit për arsimin e lartë, në fushën e teknologjive të informacionit dhe komunikimit (ICT) ose në fusha të tjera, të lidhur me njohuritë e përcaktuara në shkronjën “b” të kësaj pike;

iii. të mos jenë dënuar me vendim gjyqësor të formës së prerë për kryerjen e një vepre penale;

iv. të plotësojnë kriteret e integritetit e të besueshmërisë në ruajtjen e konfidencialitetit dhe të integritetit të informacionit, si dhe të pastërtisë së figurës;

b) Kriete profesionale:

i. të kenë përvojë pune të paktën 7 (shtatë) vjet në profesion;

ii. të kenë aftësi profesionale në fushën e sigurisë kibernetike dhe teknologjisë së informacionit;

iii. të zotërojnë njohuri të thelluara në fushën e sigurisë kibernetike dhe të teknologjisë së informacionit, si më poshtë vijon:

- njohuri për sistemet kompjuterike, virtuale dhe sistemet e operimit, si: Linux, Windows Server, sistemet virtuale, si VMWARE ose KVM, HyperV etj.;

- njohuri për protokollat e rrjeteve kompjuterike;

- njohuri për aplikacionet dhe platformat, që përdoren në rrjetet e sistemet e informacionit;

- njohuri për fushën e sigurisë së informacionit;

- taktikat, teknikat dhe procedurat (TTPs) e sulmeve kibernetike dhe aplikacioneve, që përdoren për këtë qëllim;

- njohuri mbi teknikat e hetimit kibernetik (*forensic*);

- njohuri në menaxhimin e incidenteve dhe mbrojtjen e të dhënave personale, si Log Analyst apo SIEM etj.;

- njohuri për menaxhimin e krizave kibernetike;

- njohuri në *Python*, gjuhët *Object Oriented*;

- njohuri në inteligjencën artificiale/AI, *Machine Learning*, *Blockchain*, *Cryptography*, *Autonomous Vehicles/Machines* etj.;

c) Për të vërtetuar kriteret e përcaktuara në shkronjat “a” dhe “b, të pikës 5, të këtij kreu, aplikuesi duhet të dorëzojë dokumentacionin e mëposhtëm:

i. mjet identifikimi (kopje e kartës së identitetit/pasaportës biometrike);

ii. dëshmi penaliteti, vërtetime nga gjykata që nuk është në proces gjyqësor dhe nga prokuroria që nuk është në procedim penal, si dhe vetëdeklarim që vërteton gjendjen penale;

iii. kopje të diplomës;

iv. kopje të librezës së punës ose një vërtetim nga organet tatimore, ku të jetë shënuar përvoja në profesion;

v. jetëshkrim me përvojat profesionale (CV);

vi. vetëdeklarim për integritetin dhe besueshmërinë në ruajtjen e konfidencialitetit dhe integritetit të informacionit;

vii. kopje të certifikimeve në fushën e sigurisë kibernetike dhe teknologjisë së informacionit;

viii. përbën avantazh paraqitja e certifikimeve, si vijon:

- certifikime në administrim rrjetesh dhe menaxhim sistemesh;

- certifikim në administrim të sistemeve të sigurisë së informacionit;

- certifikim profesional të sigurisë kibernetike, të tilla si: Security+, CISA, CISSP, CISM, CEH, OSCP, CHFI ose ekuivalente;

- certifikime për menaxhimin e incidenteve kibernetike;

- certifikime për investigimin e incidenteve dhe ekzaminimin digjital;

- certifikime në inteligjencën artificiale/AI;

- certifikime në *Machine Learning*;

- certifikime në *Blockchain*;

- certifikime në *Cryptography*;

- certifikime në *Autonomous Vehicles/Machines*;

- certifikime me fokus në sigurinë kibernetike të sistemeve industriale dhe kritike (SA/IEC *Cybersecurity Expert*);

- certifikime në mbrojtjen e sistemeve OT dhe ICS (GIAC *Global Industrial Cyber Security Professional*);

- certifikim për arkitekturën dhe sigurinë e sistemeve SCADA (*Certified SCADA Security Architect*);

- çdo certifikim tjetër të vlefshëm për menaxhimin e incidenteve të sigurisë kibernetike;

ç) Dokumentacioni i kërkuar në shkronjën “c”, të pikës 5, të këtij kreu, duhet të paraqitet në kopje origjinale ose të njësuar me origjinalin.

6. AKSK-ja, brenda 1 (një) jave nga hyrja në fuqi e këtij vendimi, publikon në faqen e saj zyrtare thirrjen për pjesëmarrje të ekspertëve të sigurisë kibernetike, të teknologjisë së informacionit dhe ekspertëve OT, me qëllim hartimin e listës së ekspertëve të sigurisë kibernetike, teknologjisë së informacionit dhe ekspertëve OT, të cilët do të jenë pjesë e CERT-it, ndërsa për ekspertët ndërkombëtarë thirrja do të publikohet edhe në faqet zyrtare të forumeve ndërkombëtare të sigurisë kibernetike.

7. Shpallja do të përmbajë një informacion të detajuar, në lidhje me kriteret që duhet të plotësojnë ekspertët e sigurisë kibernetike, të teknologjisë së informacionit dhe ekspertët OT, dokumentet që duhet të dorëzojnë, mënyrën dhe formën e dorëzimit të tyre.

8. Shpallja do të qëndrojë e hapur për një periudhë njëmuajore.

9. Pas paraqitjes së dokumentacionit pranë AKSK-së, kjo e fundit, brenda një afati 30-ditor, do të bëjë vlerësimin e tij bazuar në plotësimin e kriterëve të përcaktuara në këtë vendim, si dhe në procesin e intervistimit e më pas do të njoftojë ekspertët e përzgjedhur.

10. AKSK-ja do të hartojë listën me emrat dhe kontaktet e ekspertëve të sigurisë kibernetike, të teknologjisë së informacionit dhe ekspertët OT, nga të cilët do të përzgjidhen ekspertët që do të jenë pjesë e CERT-it.

11. Ekspertët, pjesë e listës së CERT-it, të cilët, në përmbushje të detyrave të tyre sipas përcaktimeve të këtij vendimi, do të kenë akses në sistemet e komunikimit e të informacionit të akredituara, ku trajtohet informacion i klasifikuar, kanë detyrimin për të ndjekur procedurat për pajisjen me “Certifikatë të sigurisë së personelit”, në përputhje me parashikimet e legjislacionit për informacionin e klasifikuar.

12. AKSK-ja do të kryejë thirrjen për ekspertë të sigurisë kibernetike, të teknologjisë së informacionit dhe ekspertë OT brenda muajit janar të çdo viti.

II. MËNYRA E ORGANIZIMIT DHE FUNKSIONIMIT TË EKIPIT TË PËRGJIGJES NDAJ EMERGJENCAVE DHE KRIZËS SË SIGURISË KIBERNETIKE

1. CERT-i mblidhet nga AKSK-ja në rast emergjence dhe krize kibernetike për hartimin e planit të masave, menaxhimin dhe zgjidhjen e emergjencës e të krizës kibernetike.

2. Mbledhjet e CERT-it drejtohen nga drejtori i përgjithshëm i AKSK-së dhe, në mungesë të tij, nga një drejtor me profil teknik nga AKSK-ja.

3. Pranë CERT-it ngrihet e funksionon sekretariati teknik i CERT-it, i cili është përgjegjës për përgatitjen e materialeve të mbledhjes dhe për njoftimin e anëtarëve të CERT-it për mbledhjen. Përbërja e sekretariatit teknik të CERT-it përcaktohet me urdhër të drejtorit të përgjithshëm të AKSK-së.

4. Në situatat e emergjencave dhe të krizave kibernetike, komunikimi ndërinstitucional mbahet duke përdorur kanalet zyrtare të komunikimit, kanalet alternative, si dhe ato rezervë (*backup*). Sekretariati teknik mban procesverbalin e takimeve, minutat e takimit, ruan përmbajtjen e komunikimeve, të njoftimeve apo të kërkesave të marra e të dhëna përmes përdorimit të mjeteve të teknologjisë së informacionit.

5. Për përballimin e emergjencave dhe të krizave kibernetike, me kërkesë të CERT-it, mund të angazhohen edhe ekspertë të sigurisë kibernetike, të teknologjisë së informacionit dhe ekspertë OT nga institucione të tjera shtetërore, sipas fushës së përgjegjësisë së tyre, për t’iu përgjigjur emergjencave dhe krizave kibernetike, sipas sektorëve përkatës.

III. FUNKSIONET E EKIPIT TË PËRGJIGJES NDAJ EMERGJENCAVE DHE KRIZËS SË SIGURISË KIBERNETIKE

Funksionet e CERT-it janë, si më poshtë vijon:

- a) Harton planin e masave të emergjencës e të krizës kibernetike;
- b) Menaxhon dhe zgjidh emergjencat e krizën kibernetike, duke ruajtur në çdo kohë konfidencialitetin;
- c) Ofron mbështetje për hartimin e rekomandimeve për të rikthyer në normalitet sistemet dhe rrjetet e informacionit në infrastrukturën e informacionit pas një incidenti në shkallë të gjerë dhe gjendjes së emergjencës e të krizës kibernetike.

IV. DISPOZITË E FUNDIT

Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike dhe institucionet e përmendura në shkronjën “a”, të pikës 2, të kreut I, për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama