REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

UDHËZIM

PËR

METODOLOGJINË E PËRCAKTIMIT TË DËNIMEVE ADMINISTRATIVE NË PROCESIN E KONTROLLIT TË INFRASTUKTURAVE KRITIKE DHE TË RËNDËSISHME TË INFORMACIONIT

Miratohet
Drejtori i Përgjithshëm

Igli TAFA

REPUBLIKA E SHQIPËRISË - AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE - KËSHILLI I MINISTRAVE

Nr. 179 Prot., Datë 03.03.2023

Tiranë 2023

Tabela e Përmbajtjes

I. Qëllimi

Ky udhëzim përcakton rregullat e përgjithshme bazë mbi metodologjinë e përcaktimit të dënimeve administrative në zbatim të Ligjit Nr. 2/2017, "Për sigurinë kibernetike", Ligjit Nr.10433, datë 16. 06. 2011, "Për inspektimin në Republikën e Shqipërisë", Ligjit Nr.10279, datë 20.05.2010, "Për kundërvajtjet administrative" si dhe "Rregullores mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë" (Version 2.0) miratuar me Urdhër nr.10, datë 14.02.2022, të Drejtorit të Përgjithshëm të AKCESK.

II. Rregulla të përgjithshme

1. Shkelja e kërkesave ligjore që konstatohen nga grupi i kontrollit, kur nuk përbën kundërvajtje penale, përbën kundërvajtje administrative, për të cilat vendoset dënimi administrativ përkatës.
2. "Dënim administrativ" është masa e paralajmërimit, gjoba dhe çdo masë apo sanksion tjetër administrativ, të parashikuara në ligjet e mësipërme, apo aktet e tjera nënligjore.
3. Në përcaktimin e dënimit apo të masës që duhet marrë, grupi i kontrollit, në përputhje me rëndësinë e shkeljeve të konstatuara apo pasojave të tyre, duke respektuar parimin e proporcionalitetit, vendos atë sanksion apo merr atë masë që është e domosdoshme dhe e përshtatshme për arritjen e qëllimit të dënimit apo masës, dhe që cenon më pak të drejtat apo interesat e ligjshme të subjektit të kontrolluar.

III. Llojet e dënimeve administrative

1. Për shkak të shkeljeve të konstatuara të kërkesave ligjore të subjektit të kontrolluar, ato klasifikohen si kundërvajtje administrative për të cilat parashikohen dënimet administrative:
   a) Dënim administrativ kryesor
   b) Dënim administrativ plotësues

Dënimi administrativ kryesor përfshin:

- Paralajmërimin e subjektit, i cili mund të shoqërohet drejtpërdrejt me një dënim tjetër kryesor administrativ më të rëndë
- Dënim me gjobë

Dënimi administrativ plotësues përfshin:

Çdo masë apo sanksion tjetër administrativ të natyrave të tjera, që shoqëron dënimin kryesor:

- Rehabilitimin dhe ndreqje e shkeljes së kërkesës ligjore.

Dënimi administrativ kryesor mund të jepet veç, por edhe bashkë me dënime administrative plotësuese. Për të njëjtën shkelje mund të vendoset një dënim kryesor dhe një apo më shumë dënime plotësuese.

Dënimi administrativ, kur është e nevojshme, shoqërohet edhe me urdhërimin e subjektit të kontrolluar për të korrigjuar shkeljet e konstatuara dhe për të eliminuar pasojat e tyre, duke përcaktuar dhe një afat të arsyeshëm kohor për këtë qëllim. Në përcaktimin e afatit, grupi i kontrollit merr në konsideratë rëndësinë e shkeljes, pasojat e saj dhe rrethanat konkrete që përcaktojnë kohën e nevojshme për kryerjen e veprimeve për këtë qëllim, me përpjekjet maksimale nga ana e subjektit të kontrolluar.

Për shkeljen e kërkesave ligjore, për çdo rast, do të zgjidhet dënimi administrativ i përshtatshëm, sipas legjislacionit në fuqi dhe duhet të jetë i mjaftueshëm për të arritur zgjidhjen e shpejtë të shkeljes, për të penguar përsëritjen e saj në të ardhmen, si dhe mungesën e bashkëpunimit nga ana e subjektit të kontrolluar.

IV. Kriteret për caktimin sipas llojit të masës së dënimit administrativ

Dënimi administrativ kryesor "***Paralajmërim***"

1. Dënimi administrativ kryesor "Paralajmërim" merret kur grupi i kontrollit, konstaton shkelje të kërkesave ligjore, që përbën kundërvajtje administrative, por që konsiderohet me risk të ulët, apo për të cilën ligji nuk parashikon dënimin përkatës administrativ.
   - "Paralajmërimi" jepet në rastet kur subjekti, nuk i plotëson masat e sigurisë organizative dhe teknike sipas përcaktimeve në Ligjin Nr. 2/2017, "Për sigurinë kibernetike", si dhe në "Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë" në **nivelin 0-9%**

2. Subjekti i kontrolluar i dënuar me dënimin administrativ "Paralajmërim" mund të dënohet drejtpërdrejt me një dënim tjetër kryesor administrativ, më të rëndë, të parashikuar në ligjin e posaçëm, kur:
   a) nuk zbaton plotësisht dhe brenda afatit të përcaktuar masat korrigjuese te konstatuara
   b) përsërit shkeljen e kërkesave ligjore

Dënimi administrativ kryesor "***Gjobë***"

1. Dënimi administrativ "Gjobë", është dënim administrativ kryesor, i cili i jepet subjektit të kontrolluar kur nuk plotëson kërkesat ligjore të përcaktuara në ligjin nr. 2/2017 "Për Sigurinë Kibernetike" si dhe në "Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë".

Masa e gjobës është e shprehur me intervale sipas pikëve të grumbulluara, përqindjes (%) së përmbushjes së masave të sigurisë kibernetike, si dhe vlerësimit të nivelit të riskut.

V. Rastet e dënimit administrativ

A. Operatorët e Infrastrukturave Kritike dhe Operatorët e Infrastrukturave të Rëndësishme të Informacionit

1. Mosraportimi i incidenteve kibernetike, në zbatim të pikës 1, të nenit 11, të ligjit nr. 2/2017 "Për sigurinë kibernetike", përbën, kundërvajtje administrative dhe sanksionohen me gjobë, në vlerë nga 200 000 (dyqind mijë) deri në 800 000 (tetëqind mijë) lekë;

2. Mospërmbushja e detyrimeve për nëpunësit e Autoritetit, që marrin pjesë në zgjidhjen e incidentit të sigurisë kibernetike, të ruajnë konfidencialitetin e plotë për të gjitha të dhënat e përpunuara gjatë procedurës së zgjidhjes së incidentit. Konfidencialiteti duhet të ruhet edhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin, përveç rasteve të parashikuara në ligj, përbën, kundërvajtje administrative dhe sanksionohen me gjobë, në vlerë nga nga 40 000 (dyzet mijë) lekë deri në 200 000 (dyqind mijë) lekë;

3. Mosraportimi pranë Autoritetit i pikës së kontaktit apo i përditësimeve të tyre, në zbatim të pikës 4, të nenit 18, të ligjit nr. 2/2017 "Për sigurinë kibernetike" përbën, kundërvajtje administrative dhe sanksionohen me gjobë, në vlerë nga 20 000 (njëzet mijë) lekë deri në 40 000 (dyzet mijë) lekë;

4. Mospërmbushja e detyrimeve të përcaktuara në kuadër të masave korrigjuese, në zbatim të nenit 20 të ligjit nr. 2/2017 "Për sigurinë kibernetike", përbën, kundërvajtje administrative dhe sanksionohen me gjobë, në vlerë nga 200 000 (dyqind mijë) deri në 800 000 (tetëqind mijë) lekë;

VI. Përcaktimi i vlerës të gjobës

1. AKCESK do të përcaktojë vlerën e gjobës brenda kufirit maksimal dhe minimal të vendosur në ligjin nr. 2/2017 "Për sigurinë kibernetike"

Kriteret e përcaktimit të vlerës të gjobës bazohen në:

a) Përqindjen (%) e përmbushjes së masave teknike dhe organizative të sigurisë kibernetike, të përcaktuara në ligjin nr. 2/2017 "Për sigurinë kibernetike", si dhe në rregulloren "Mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë";
b) Nivelin e riskut të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit.
c) Kategorinë e incidenteve Kibernetike
d) Nëse kundërvajtësi rezulton i dënuar administrativisht edhe më parë;

VII. Metodologjia e përcaktimit të dënimeve administrative për mospërmbushjen e detyrimeve të raportimit të incidenteve kibernetike nga Operatorët e Infrastrukturave Kritike dhe Operatorët e Infrastrukturave të Rëndësishme të Informacionit

1. Operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave së rëndësishme të informacionit janë të detyruar të raportojnë menjëherë pasi zbulojnë incidentet e sigurisë kibernetike pranë Autoritetit;
2. Subjektet të cilët nuk raportojnë incidentet kibernetike pranë Autoritetit, sipas kategorive të incidenteve, si dhe brenda kohës së përcaktuar për raportim, bazuar në Ligjin nr.2/2017 "Për Sigurinë Kibernetike", si dhe në Rregulloren "Për kategoritë e incidenteve kibernetike si dhe formatin e elementët e raportit" (Miratuar me urdhër nr.62 ,datë 10.09.2018), do të sanksionohen me gjobë në bazë të:
   a. Kategorisë së incidentit kibernetik
   b. Kategorizimit të infrastrukturës (kritike/e rëndësishme)
   c. Vlerësimit të nivelit te riskut
   d. Kohës së përcaktuar të raportimit

Kategoria	"Sistem Kritik"			"Sistem i Rëndësishëm"		
	Koha e raportimit	**Niveli i Riskut**	**Masa Administrative**	**Koha e raportimit**	**Niveli Riskut**	**Masa Administrative**
Kategoria 1 Compromised Information	Brenda 4 orësh nga zbulimi	I Lartë	400 000	Brenda 24 orësh nga zbulimi	I Mesëm	200 000
Kategoria 2 Compromised Asset	Brenda 4 orësh nga zbulimi	I Lartë	400 000	Brenda 24 orësh nga zbulimi	I Mesëm	200 000
Kategoria 3 Unauthorised Access	Brenda 4 orësh nga zbulimi	I Lartë	400 000	Brenda 24 orësh nga zbulimi	I Mesëm	200 000
Kategoria 4 Malicious Code	Brenda 4 orësh nga zbulimi nëse është shpërndarë në gjithë institucionin	Shumë i Lartë	800 000	Brenda 24 orësh nga zbulimi nëse është shpërndarë në gjithë institucionin	I Lartë	600 000
Kategoria 5 Intrusions against networks	Brenda 4 orëve nga zbulimi nëse sulmi është duke vazhduar dhe institucioni nuk është në gjendje ta ndalojë atë	I Lartë	400 000	Brenda 24 orësh nga zbulimi nëse sulmi është duke vazhduar dhe institucioni nuk është në gjendje ta ndalojë atë	I Mesëm	200 000
Kategoria 6 Phishing or Social Engineering	Brenda 4 orësh nga zbulimi	I Lartë	400 000	Brenda 24 orësh nga zbulimi	I Mesëm	200 000

Kategoria 7 Unlawful activity	Brenda 4 orësh nga zbulimi	I Lartë	600 000	Brenda 24 orësh nga zbulimi	I Mesëm	300 000
Kategoria 8 Scans/Probes/ Attempted Access	Brenda 4 ore nga zbulimi	I Ulët	200 000	Brenda 24 orësh nga zbulimi	I Ulët	200 000
Kategoria 9 Policy Violations	Brenda 4 orësh nga zbulimi	I Lartë	400 000	Brenda 24 orësh nga zbulimi	I Mesëm	200 000
Kategoria 10 Theft/loss of assets	Brenda 4 orësh nga zbulimi	I Lartë	600 000	Brenda 24 orësh nga zbulimi	I Mesëm	300 000
Kategoria 11 Unauthorised release of or disclosure of information	Brenda 1 orë nga zbulimi	Shumë i Lartë	800 000	Brenda 2 orësh nga zbulimi	I Lartë	600 000

Në rast të shkeljeve ligjore të përsëritura, aplikohet **2-fishi** i masës së gjobës, por jo më shumë se vlera maksimale e përcaktuar në nenin 22, shkronja a, të ligjit nr.2/2017 "Për sigurinë Kibernetike"

VIII. Metodologjia e përcaktimit të dënimeve administrative për mospërmbushjen e detyrimeve për nëpunësit e Autoritetit, për ruajtjen e Konfidencialiteti i të dhënave gjatë procedurës së zgjidhjes së incidentit kibernetik

1. Bazuar në pikën 1, të nenit 13, të ligjit nr. 2/2017 "Për sigurinë kibernetike", nëpunësit e Autoritetit, që marrin pjesë në zgjidhjen e incidentit të sigurisë kibernetike, janë të detyruar të ruajnë konfidencialitetin e plotë për të gjitha të dhënat e përpunuara gjatë procedurës së zgjidhjes së incidentit. Konfidencialiteti duhet të ruhet edhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin, përveç rasteve të parashikuara në ligj.

2. Nëpunësit e Autoritetit të cilët nuk përmbushin detyrimin e përcaktuar në paragrafin 1, sanksionohen me gjobë si më poshtë:

    a. 200 000(dyqind mijë) lekë, për mosruajtjen e konfidencialitetit të plotë për të gjitha të dhënat të konsideruara të nivelit "**Sekret**" e përpunuara gjatë procedurës së zgjidhjes së incidentit në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin
    b. 100 000(njëqind mijë) lekë, për mosruajtjen e konfidencialitetit të plotë për të gjitha të dhënat të konsideruara të nivelit "**Konfidencial**" e përpunuara gjatë procedurës së zgjidhjes së incidentit në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin
    c. 40 000 (dyzet mije), për mosruajtjen e konfidencialitetit të plotë për të gjitha të dhënat të konsideruara të nivelit "**i Kufizuar**" e përpunuara gjatë procedurës së zgjidhjes së

incidentit në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin

IX. Metodologjia e përcaktimit të dënimeve administrative për mosraportim pranë Autoritetit i pikës së kontaktit apo i përditësimeve të tyre

1. Bazuar në nenin 18, të ligjit nr. 2/2017 "Për sigurinë kibernetike", Operatorët e infrastrukturës kritike të informacionit dhe operatorët e infrastrukturës së rëndësishme të informacionit caktojnë pikat e kontaktit, të dhënat e të duhet ti raportohen Autoritetit. Në rastet e ndryshimeve në të dhënat e pikave të kontaktit i komunikohen Autoritetit brenda 7 ditëve kalendarike.
2. Mosraportimi pranë Autoritetit i pikës së kontaktit apo i përditësimeve të tyre, në zbatim të paragrafit 1, përbën, kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë:
   a) mosraportimi i pikës së kontaktit nga Operatorët e Infrastrukturave Kritike të Informacionit(OIKI) apo i përditësimeve të tyre, dënohet me gjobe me vlerën me 40 000(dyzet mijë) Lekë.
   b) mosraportimi i pikës së kontaktit nga Operatorët e Infrastrukturave të Rëndësishme të Informacionit(OIRI) si dhe ndryshimi i tyre dënohet me gjobe me vlerën me 20 000(njëzet mijë) Lekë.

X. Metodologjia e përcaktimit të dënimeve administrative për mospërmbushjen e detyrimeve të masave korrigjuese në kuadër të implementimit të masave të sigurisë kibernetike nga Operatorët e Infrastrukturave Kritike të Informacionit dhe Operatorët e Infrastrukturave të Rëndësishme të Informacionit

1. Subjektet që kanë kryer shkelje të kërkesave ligjore të identifikuara sipas listës së mëposhtme të treguesve, do të penalizohen në bazë të pikëve të grumbulluara, të konvertuara në përqindje (%) të mospërmbushjes së masave të sigurisë, si dhe vlerësimit të nivelit të riskut.

2. Sipas kësaj metodologjie secila masa e sigurisë ka **5 pikë** dhe totali është **100 pikë** për të gjitha masat organizative dhe teknike të përcaktuara në Ligjin Nr. 2/2017, "Për sigurinë kibernetike", si dhe në "Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë".

3. Në fund të kontrollit mblidhen të gjitha pikët e grumbulluara për secilën masë sigurie. Sipas pikëve të grumbulluara llogaritet përqindja (%) e përmbushjes së masave të sigurisë kibernetike nga OIKI dhe OIRI si dhe vlerësohet niveli i riskut (*i ulët, i mesëm, i lartë),* bazuar në implementimin e masave të sigurisë në infrastrukturën e tyre.

Në varësi të % së përmbushjes së masave të sigurisë nga Operatorët e Infrastrukturave Kritike të Informacionit dhe Operatorët e Infrastrukturave të Rëndësishme të Informacionit, si dhe nivelit të vlerësuar të riskut, behet penalizimi i subjektit me dënimin administrativ si më poshtë:

Mospërmbushja e masave të sigurisë në nivelin 0-9%, penalizohet me dënimin administrativ "paralajmërim"
Mospërmbushja e masave të sigurisë në nivelin 10% - 19% penalizohet me gjobë 200 000 lekë
Mospërmbushja e masave të sigurisë në nivelin 20% -29% penalizohet me gjobë 300 000 lekë

Mospërmbushja e masave të sigurisë në nivelin 30% -39%penalizohet me gjobë 400 000 lekë
Mospërmbushja e masave të sigurisë në nivelin 40% - 49%penalizohet me gjobë 500 000 lekë
Mospërmbushja e masave të sigurisë në nivelin 50% - 59%penalizohet me gjobë 600 000 lekë
Mospërmbushja e masave të sigurisë në nivelin 60% - 69%penalizohet me gjobë 700 000 lekë
Mospërmbushja e masave të sigurisë në nivelin 70% - 100% penalizohet me gjobë 800 000 lekë

	Domain	**Piket**	**Vlerësimi**
Nr.	**Masat Organizative**		
1	Politika e sigurisë	5	
2	Menaxhimi i riskut	5	
3	Siguria Organizative	5	
4	Kërkesat e sigurisë për palët e treta	5	
5	Sigurisë e burimeve njerëzore dhe aksesit të personave	5	
6	Menaxhimi i aseteve	5	
7	Ngjarjet e sigurisë e të menaxhimit të incidenteve të sigurisë kibernetike	5	
8	Menaxhimi i vazhdimësisë së punës	5	
9	Menaxhimi i sigurisë së informacionit	5	
10	Kontrolli dhe auditi	5	
	Masat Teknike		
1	Siguria fizike	5	
2	Menaxhimi për autorizimin e aksesit	5	
3	Pajisjet kriptografike	5	
4	Zbulimi i ngjarjeve të sigurisë kibernetike	5	
5	Mjetet e gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike	5	
6	Mbrojtja e integritetit të rrjeteve të komunikimit	5	
7	Verifikimi i identitetit të përdoruesve	5	
8	Veprimtaria e administratorëve dhe përdoruesve	5	
9	Siguria e aplikacioneve	5	
10	Siguria e sistemeve industriale	5	
	Totali	100	

% e përmbushjes së masave të sigurisë	**Vlerësimi i nivelit të Riskut**	**Masa administrative**
91% -100%	I Ulët	Paralajmerim
81% - 90%	I Ulët	200 000 lekë
71% - 80%	I Ulët	300 000 lekë
61% - 70%	I Mesëm	400 000 lekë
51% - 60%	I Mesëm	500 000 lekë
41% - 50%	I Lartë	600 000 lekë
31% - 40%	I Lartë	700 000 lekë
0% - 30%	I Lartë	800 000 lekë

Në rast të shkeljeve ligjore të përsëritura, aplikohet **2-fishi** i masës së gjobës, por jo më shumë se vlera maksimale e përcaktuar në nenin 22, shkronja ç, të ligjit nr.2/2017 "Për sigurinë Kibernetike"

XI. Ankimimi i vendimeve për dënimet administrative

1. Kundër vendimit të dënimit administrativ, kundërvajtësi mund të bëjë ankim në Gjykatën Administrative të Shkallës së Parë Tiranë, brenda 30 (tridhjetë) ditëve nga komunikimi i këtij Vendimi.
2. Në zbatim të Ligjit Nr.10279, datë 20.05.2010, "Për kundërvajtjet administrative" nenet 20, 21, 22, vendimi për dënimin administrativ përbën titull ekzekutiv.
3. Gjobat duhet të paguhen brenda 10 ditëve nga marrja në dijeni nga kundërvajtësit, pas kalimi të këtij afati gjoba ekzekutohet nga shërbimi përmbarimor.
4. Pagesa e gjobave bëhet nga kundërvajtësi ne buxhetin e shtetit , sipas faturës përkatëse të arkëtimit.