REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 2458 Prot. Tiranë, më 27.08.2025

URDHËR

Nr. 229, datë 27.08.2025

PËR MIRATIMIN E PROCEDURËS PËR KOMUNIKIMIN ME PUBLIKUN PËR INCIDENTET KIBERNETIKE QË CENOJNË INTERESIN PUBLIK

Në zbatim të shkronjës a, të pikës 1, të nenit 2 dhe nenit 99 të ligjit nr. 44/2015 "Kodi i procedurave administrative i Republikës së Shqipërisë" dhe pikës 2, të nenit 26 të ligjit nr.25/2024 "Për sigurinë kibernetike",

U R DH Ë R O J:

1.Miratimin e procedurës "Për komunikimin me publikun për incidentet kibernetike që cenojnë interesin publik", sipas tekstit bashkëlidhur këtij urdhri, pjesë përbërëse e tij.

2. Ngarkohen Drejtoria e Analizës së Sigurisë Kibernetike, Drejtoria e Monitorimit dhe Reagimit të Incidenteve, Qendrës Operacionale SOC C-SIRT dhe Drejtoria e Koordinimit të Projekteve Ndërkombëtare dhe Zhvillimit Strategjik të Sigurisë Kibernetike, të Autoritetit Kombëtar për Sigurinë Kibernetike për zbatimin e këtij urdhri.

3. Ky urdhër hyn në fuqi menjëherë.

DREJTOR I PËRGJITHSHËM

Igli Tafa

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

PROCEDURA PËR KOMUNIKIMIN ME PUBLIKUN PËR INCIDENTET KIBERNETIKE QË CENOJNË INTERESIN PUBLIK

Kjo procedurë ka për qëllim të përcaktojë mënyrën e komunikimit me publikun në rastet e incidenteve kibernetike të cilat kanë ose mund të kenë ndikim në interesin publik. Ajo synon të sigurojë transparencë institucionale, informim të saktë dhe në kohë të publikut, ruajtjen e besimit të qytetarëve dhe palëve të interesuara, si dhe minimizimin e ndikimeve negative që mund të shkaktohen nga dezinformimi ose paniku i krijuar në publik.

Procedura zbatohet për të gjitha incidentet kibernetike që prekin ose rrezikojnë të prekin infrastrukturat kritike dhe të rëndësishme të informacionit, shërbimet kritike, të dhënat personale apo sensitive, si dhe funksionimin normal të shërbimeve të ofruara me rëndësi për publikun.

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, referuar ligjit nr. 25/2024 "Për sigurinë kibernetike". Incident kibernetik që cenon interesin publik konsiderohet çdo incident që prek qytetarë, përdorues, klientë ose shërbime kritike me ndikim të gjerë për publikun dhe që kërkon komunikim zyrtar me qëllim për të parandaluar përshkallëzimin e tij dhe minimizuar pasojat e incidentit.

Komunikimi me publikun në rast incidentesh kibernetike duhet të jetë i saktë, i qartë, transparent dhe me përgjegjësi. Informacioni që publikohet duhet të jetë i verifikuar, i kuptueshëm për publikun e gjerë dhe në proporcion me nivelin e rrezikut dhe ndikimit të incidentit. Ky komunikim duhet të jetë në përputhje me legjislacionin në fuqi për sigurinë kibernetike, legjislacionin në fuqi për të drejtën e informimit dhe mbrojtjen e të dhënave personale dhe legjislacionin në fuqi për informacionin e klasifikuar.

Në zbatim të pikave 1 dhe 2 të nenit 26 të ligjit nr. 25/2024 "Për sigurinë kibernetike", CSIRT-i Kombëtar pranë Autoritetit Kombëtar për Sigurinë Kibernetike, pasi është konsultuar me operatorin e infrastrukturës së informacionit, informon publikun për incidentet e ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit kur informimi është i nevojshëm për ndërgjegjësimin e publikut, për të parandaluar një incident të rëndësishëm, trajtimin e incidentit apo kur prek interesin publik, duke ruajtur gjithmonë konfidencialitetin e të dhënave të incidentit. Për realizimin e komunikimit ndiqet procedura sipas hapave të përcaktuar në këtë dokument.

PROCEDURA E KOMUNIKIMIT

Hapi 1: Konfirmimi i incidentit kibernetik

CSIRT-i Kombëtar, si struktura përgjegjëse për monitorimin, analizimin dhe menaxhimin e kërcënimeve kibernetike, vulnerabiliteteve dhe incidenteve në nivel kombëtar, konfirmon incidentin kibernetik dhe zbaton procedurën për menaxhimin e tij. Nëse pas analizës së incidentit të sigurisë kibernetike rezulton se ka ndikime të konsiderueshme për publikun si ndërprerje shërbimi, kompromentim i të dhënave personale, ndikim financiar dhe ndikime të tjera që prekin interesin publik, Autoriteti vijon me informimin e publikut nëpërmjet kanaleve zyrtare të komunikimit, pasi është konsultuar me operatorin e infrastrukturës së informacionit.

Hapi 2: Përgatitja e njoftimit fillestar për publikun

Autoriteti përgatit njoftimin fillestar i cili përmban një përshkrim të përgjithshëm të incidentit, shërbimet ose kategoritë e përdoruesve dhe qytetarëve të prekur, masat e ndërmarra për menaxhimin e situatës dhe, nëse është e nevojshme, informacion mbi hapat e mëtejshëm. Ky njoftim synon të informojë publikun mbi incidentin dhe masat emergjente që duhen marrë për minimizimin e rrezikut, pa zbuluar detaje që mund të rrezikojnë sigurinë ose analizën e incidentit, si dhe të parandalojë krijimin e panikut për qytetarët.

Hapi 3: Përditësimi i vazhdueshëm mbi situatën

Kur vlerësohet e nevojshme, gjatë menaxhimit të incidentit, Autoriteti bën përditësim të informacionit për publikun, në varësi të zhvillimit të situatës dhe nivelit të interesit publik. Këto përditësime përfshijnë informacion mbi progresin e zgjidhjes së incidentit, masat shtesë të sigurisë të ndërmarra dhe, kur është e nevojshme, rekomandime praktike për qytetarët ose subjektet e prekura.

Hapi 4: Publikimi i raportit mbi incidentin dhe njoftimit përfundimtar

Pas finalizimit të raportit të analizës së incidentit kibernetik, Autoriteti publikon raportin në faqen zyrtare. Në rastet kur ky raport përmban të dhëna sensitive, kryhet procesi i anonimizimit të të dhënave para publikimit të tij. Gjithashtu, publikohet edhe një njoftim përfundimtar, i cili paraqet një përmbledhje të incidentit, vlerësimin e ndikimit dhe rekomandimet për të shmangur incidente të ngjashme në të ardhmen.

Komunikimi me publikun realizohet përmes kanaleve zyrtare të institucionit, që përfshijnë si më poshtë vijon:

- faqen zyrtare *web*;
- rrjetet sociale të institucionit;
- deklarata për shtyp, sipas rastit.

Autoriteti identifikon informacionet e pasakta ose dezinformuese në media dhe rrjete sociale në lidhje me incidentin dhe ndërmerr masa për korrigjimin e tyre përmes komunikimeve zyrtare dhe të koordinuara.