



REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 1016 Prot

Tiranë më 07.11.2024

URDHËR

Nr. 408 datë. 07.11. 2024

PËR
MIRATIMIN E RREGULLORES “PËR MËNYRAT DHE AFATET E RUAJTJES SË
LOG-EVE TË INCIDENTEVE TË SIGURISË KIBERNETIKE”

Në zbatim të nenit 13 shkronja “f”, nenit 16 shkronja “ç”, si dhe nenit 17 shkronja “dh” të ligjit
nr. 25/2024 “Për sigurinë kibernetike”,

URDHËROJ:

1. Miratimin e rregullores “Për mënyrat dhe afatet e ruajtjes së log-eve të incidenteve të sigurisë kibernetike” sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, CSIRT-et sektoriale, si dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI Tafa





REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

RREGULLORE

**PËR MËNYRAT DHE AFATET E RUAJTJES SË LOGEVE TË INCIDENTEVE TË
SIGURISË KIBERNETIKE**

PËRMBAJTJA	faqe
KREU I: DISPOZITA TË PËRGJITHSHME.....	3
Objekti dhe qëllimi	3
Baza ligjore.....	3
Fusha e zbatimit.....	3
Rolet dhe përgjegjësitë.....	3
Përkufizime.....	4
KREU II: MËNYRAT, AFATET DHE AKSESI NË RUAJTJEN E LOGEVE	4
Mënyrat e ruajtjes së logeve të incidenteve	4
Mbrojtja e log-eve të incidenteve	5
Aksesi në hapësirat e ruajtjes së logeve.....	5
Afatet e ruajtjes së log-eve të incidenteve.....	6
KREU III: SHKATËRRIMI I LOG-EVE TË INCIDENTEVE	7
Shkatërrimi i log-eve të incidenteve.....	7
KREU IV: PAJTUESHMËRIA DHE TRAJNIMET.....	7
Pajtueshmëria	7
Trajnimi i personelit.....	7

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1

Objekti dhe qëllimi

Objekti i kësaj rregulloreje është përcaktimi i procedurave dhe afateve për ruajtjen e logeve të incidenteve të sigurisë kibernetike të evidentuara nga CSIRT-i pranë operatorit dhe të raportuara pranë CSIRT-i sektorial dhe ai Kombëtar, me qëllim ruajtjen e sigurt, mbrojtjen, aksesin dhe shkatërrimin e tyre.

Neni 2

Baza ligjore

Kjo rregullore është hartuar në zbatim nenit 13 shkronja “f”, nenit 16 shkronja “ç”, si dhe nenit 17 shkronja “dh” të ligjit nr. 25/2024 “Për sigurinë kibernetike”.

Neni 3

Fusha e zbatimit

Kjo rregullore është e detyrueshme të zbatohet nga CSIRT-i pranë operatorit, CSIRT-i sektorial dhe CSIRT-i Kombëtar lidhur me log-et e incidenteve të sigurisë kibernetike të krijuara, të ruajtura, të aksesuara dhe të shkatërruara në hapësirën digjitale dhe fizikë.

Neni 4

Rolet dhe përgjegjësitë

Rolet dhe përgjegjësitë e CSIRT-it Kombëtar, CSIRT-it sektorial dhe atij pranë operatorit në ruajtjen e logeve të incidenteve të sigurisë kibernetike në zbatim të kësaj rregulloreje janë si më poshtë vijon:

1. CSIRT-it Kombëtar si Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike siguron log-et e incidenteve nga raportimet e CSIRT-it pranë operatorit dhe në këtë kuadër ka detyrimin e ruajtjes së këtyre log-eve sipas mënyrës dhe afateve të përcaktuara në këtë rregullore.

2. CSIRT-it Sektorial si Ekipi i Përgjigjes për Incidentet e Sigurisë Kibernetike për sektorin përkatës siguron logjet e incidenteve nga raportimet e CSIRT-it pranë operatorit dhe në këtë kuadër ka detyrimin e ruajtjes së këtyre logeve sipas mënyrës dhe afateve të përcaktuara në këtë rregullore.
3. CSIRT-it pranë operatorit si Ekipi i Përgjigjes ndaj Incidenteve të Sigurisë Kibernetike siguron logjet e incidenteve nga zbulimi i incidenteve të sigurisë kibernetike pranë infrastrukturave të informacionit dhe në këtë kuadër ka detyrimin e ruajtjes së këtyre logeve sipas mënyrës dhe afateve të përcaktuara në këtë rregullore.

Neni 5

Përkufizime

Termat e përdorura në këtë rregullore kanë të njëjtin kuptim me termat e përcaktuara në ligjin nr.25/2024 “Për sigurinë kibernetike”, ndërsa termat e mëposhtëm kanë këto kuptime:

1. “CIA”, i referohet konfidencialitetit, integritetit dhe disponueshmërisë në bazë të parimit të mbrojtjes së informacionit dhe të dhënave sensitive nga kërcënimet dhe rreziqet e mundshme të sigurisë kibernetike.
2. “AAA”, i referohet autentifikimit, autorizimit dhe llogaridhënies për të siguruar një kontroll të plotë të aksesit dhe monitorimin e aktiviteteve në sistemet e informacionit.
3. “RBAC”, i referohet metodës për të menaxhuar aksesin në sisteme duke përdorur role, ku çdo rol është një grup privilegjesh që mund të caktohen për përdoruesit në sistem.

KREU II

MËNYRAT, AFATET DHE AKSESI NË RUAJTJEN E LOGEVE

Neni 6

Mënyrat e ruajtjes së logeve të incidenteve

Logjet e incidenteve të sigurisë kibernetike ruhen në hapësirë digjitale dhe hapësirë fizike.

1. Ruajtja e logeve në hapësirë digjitale duhet të bëhet në përputhje me përcaktimet e mëposhtme:
 - a) Logjet e incidenteve duhet të ruhen nga CSIRT-i pranë operatorit, CSIRT-i Sektorial dhe nga CSIRT-i Kombëtar të mbështetur në parimin CIA. Gjithashtu logjet mund të ruhen dhe në një **sistem qendror** të menaxhuar nga CSIRT-i Kombëtar.
 - b) Aksesin në sistemin e ruajtjes së logeve të incidenteve duhet të kufizohet vetëm për personelin e autorizuar sipas parimit AAA.

- c) “Backup-et” e log-eve duhet të ruhen në një vend të izoluar dhe të ndarë fizikisht sipas standardeve të mirënjohura ndërkombëtare.
- 2. Ruajtja e log-eve të incidenteve në hapësirën fizike duhet të bëhet në përputhje me përcaktimet e mëposhtme:
 - a) Ruajtja e log-eve të incidenteve në hapësirën fizike realizohet në një hapësirë të mbyllur, me akses të kontrolluar.
 - b) Aksesit në hapësirën fizike duhet të kufizohet vetëm për personelin e autorizuar.

Neni 7

Mbrotjtja e log-eve të incidenteve

Për të siguruar mbrojtjen e log-eve të incidenteve aplikohen të gjitha proceset e mëposhtme:

1. **Enkriptimi:** Të gjithë log-et e incidenteve të ruajtura në hapësirën digjitale duhet të kodohen duke përdorur algoritme të forta enkriptimi për të garantuar konfidencialitetin dhe integritetin e të dhënave si në ruajtjen ashtu edhe në transmetimin e tyre.
2. **Kontrolli i aksesit:** Të zbatohet kontrolli i aksesit në log-et e incidenteve të bazuar në role (RBAC) për të siguruar që vetëm personeli i autorizuar mund t’i aksesojë ato.
3. **Monitorimi:** Sistemi i ruajtjes së logeve duhet të monitorohet në mënyrë të vazhdueshme, minimumi dy herë në vit, për të identifikuar aksesin e paautorizuar në to.
4. **Disponueshmëria:** Të garantohet siguria dhe aksesueshmëria e log-eve të incidenteve të sigurisë kibernetike, në mënyrë që ato të mund të përdoren kur nevojiten, pavarësisht nga rreziqet ose ndodhitë e mundshme, si një nga komponentët kryesorë të sigurisë së informacionit.
5. **Paprekshmëria e Sistemeve dhe Aplikacioneve:** CSIRT-et duhet të garantojnë paprekshmërinë e të gjitha proceseve të sistemeve dhe aplikacioneve të cilët gjenerojnë log-e.
6. **Gjurmimi:** Procesi i gjurmimit të log-eve duhet të sigurojë mbledhjen, ruajtjen dhe analizën e informacionit të regjistruar në loge për të monitoruar aktivitetet e sistemeve dhe përdoruesve, me qëllim që këto aktivitete të jenë të gjurmueshme dhe të auditueshme në mënyrë të saktë dhe efektive për të mundësuar identifikimin, analizimin, parandalimin dhe përmirësimin në përgjigjen ndaj incidenteve të sigurisë kibernetike.
7. **Trajtimi i incidentit në rastin e shkeljes së ruajtjes së logeve:** Në rast të shkeljes së sigurisë, integritetit dhe konfidencialitetit të log-eve të incidenteve duhet të merren masa të menjëhershme sipas përcaktimeve të rregullores në fuqi për menaxhimin e incidenteve të sigurisë kibernetike.

Neni 8

Aksesi në hapësirat e ruajtjes së log-eve

1. Çdo kërkesë për të hyrë në hapësirën dixhitale dhe fizike ku ruhen loget e incidenteve të sigurisë kibernetike duhet të dokumentohet zyrtarisht dhe të miratohet nga titullari i CSIRT-it ose personi i autorizuar prej tij.
2. Të gjitha akseset në hapësirat e ruajtjes së logeve të incidenteve duhet të regjistrohen, duke përfshirë identitetin e përdoruesit, kohën e aksesit, të drejtat e përdoruesit dhe natyrën e aksesit.
3. Personeli që hyn në hapësirat e ruajtjes së log-eve të incidenteve kanë detyrimin e zbatimit të parimit të konfidencialitetit.

Neni 9

Afatet e ruajtjes së log-eve të incidenteve

Periudha e ruajtjes së log-eve nga CSIRT-et në hapësirë digjitale dhe hapësirë fizike në zbatim të kësaj rregulloreje janë si më poshtë:

1. Log-et e incidenteve që përmbajnë të dhëna personale ruhen nga CSIRT-i pranë operatorit në përputhje me afatet sipas përcaktimeve të legjislacionit në fuqi për të dhënat personale.
Log-et e incidenteve që nuk përmbajnë të dhëna personale ruhen nga CSIRT-i pranë operatorit për një afat nga 1 (një) vit deri në 3 (tre) vite, në varësi të rrezikut dhe kërkesave operacionale.
2. Log-et e incidenteve që përmbajnë të dhëna personale ruhen nga CSIRT-i sektorial në përputhje me afatet sipas përcaktimeve të legjislacionit në fuqi për të dhënat personale.
Log-et e incidenteve që nuk përmbajnë të dhëna personale ruhen nga CSIRT-i sektorial për një afat nga 1 (një) vit deri në 3 (tre) vite, në varësi të rrezikut dhe kërkesave operacionale.
3. Log-et e incidenteve që përmbajnë të dhëna personale ruhen nga CSIRT-i Kombëtar në përputhje me përcaktimet e legjislacionit në fuqi për të dhënat personale.
Loget e incidenteve që nuk përmbajnë të dhëna personale ruhen nga CSIRT-i Kombëtar për një afat nga 1 (një) vit deri në 3 (tre) vite, në varësi të rrezikut dhe kërkesave operacionale.

KREU III

SHKATËRRIMI I LOG-EVE TË INCIDENTEVE

Neni 10

Shkatërrimi i logeve të incidenteve

1. Pas kalimit të afateve të përcaktuar në nenin 9 të kësaj rregulloreje CSIRT-et kanë detyrimin e shkatërrimit të këtyre log-eve.
2. Log-et e ruajtura në hapësirën digjitale duhet të shkatërrohen me metoda të sigurta të fshirjes, si fshirja kriptografike ose mbishkrimi, duke siguruar që ato të mos rikuperohen.
3. Log-et e ruajtura në hapësirën fizike duhet të copëtohen ose të digjen për të siguruar shkatërrimin e plotë të tyre.
4. Shkatërrimi i log-eve të incidenteve duhet të dokumentohet nëpërmjet një procesverballi, në të cilin identifikohet/regjistrohet data, metoda dhe personat e përfshirë në procesin e shkatërrimit.

KREU IV

PAJTUESHMËRIA DHE TRAJNIMET

Neni 11

Pajtueshmëria

1. CSIRT-et duhet të kryejnë kontrolle të rregullta të pajtueshmërisë për të siguruar respektimin e detyrimeve të përcaktuara në këtë rregullore.
2. Të gjitha veprimet që lidhen me ruajtjen, aksesin dhe shkatërrimin e log-eve të incidenteve duhet të jenë të auditueshme, si dhe të dokumentohen nga ana e CSIRT-eve.

Neni 12.

Trajnimi i personelit

CSIRT-et duhet të kryejnë programe të rregullta trajnimi për të siguruar që i gjithë personeli i përfshirë në menaxhimin e ruajtjes së log-eve të incidenteve të jetë i vetëdijshëm për përgjegjësitë e tyre dhe procedurat e përshkruara në këtë rregullore.