



REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE
SIGURINË KIBERNETIKE

Rregullore për Kategoritë e Incidenteve Kibernetike si dhe
formatin e elementët e raportit

Miratuar me Urdhrin nr.62, datë 10.09.2018, të Drejtorit të
Përgjithshëm të Autoritetit Kombëtar për Certifikimin
Elektronik dhe Sigurinë Kibernetike (AKCESK)

Përmbajtja

<i>Hyrje</i>	2
<i>Qëllimi</i>	2
<i>Kategoritë e incidenteve kibernetike</i>	2
<i>Procedura e përshkallëzimit të incidentit kibernetik</i>	6
<i>Forma e raportimit të incidentit kibernetik</i>	8
<i>Incidente që nuk janë të nevojshme të raportohen</i>	10

Hyrje

Menaxhimi efektiv i sigurisë kibernetike përfshin një kombinim të aftësive të parandalimit, zbulimit dhe reagimit ndaj incidenteve në hapësirën kibernetike. Me qëllim arritjen e një niveli të lartë të sigurisë, një infrastrukturë kritike ose e rëndësishme e informacionit duhet të jetë në gjendje për t'iu përgjigjur incidenteve dhe të ketë të miratuara procedurat e duhura në rastin kur ndodh një incident që cënon sigurinë e informacionit.

Për një zgjidhje efikase të incidenteve potenciale të sigurisë kibernetike, është i nevojshëm kategorizimi i incidenteve kibernetike, si dhe përcaktimi i procedurës së përshkallëzimit të incidentit nga identifikimi, trajtimi deri në zgjidhjen e tij.

Kjo rregullore është hartuar në bazë të Ligjit Nr. 2 datë 26.01.2017 për “Sigurinë Kibernetike”, Neni 11 pika 2.

Qëllimi

Qëllimi i hartimit të kësaj rregulloreje është përcaktimi i kategorive të incidenteve të sigurisë kibernetike, formatin e elementët e raportit si dhe procedurën e përshkallëzimit të incidentit kibernetik.

Kategoritë e incidenteve kibernetike

Incident i sigurisë kibernetike, është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cënimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit dhe sjell një efekt real negativ.

Pasi raportohet për një incident, ai duhet të trajtohet në mënyrë efikase dhe të shpejtë deri në zgjidhjen e tij. Kategorizimi i incidenteve kibernetike ndihmon për të planifikuar veprimet për zgjidhjen e incidentit dhe ndihmon palët të respektojnë afatin kohor të raportimit, në varësi të infrastrukturës kritike ose të rëndësishme të informacionit që zotëron operatori.

Kategoria	Emri	Përshkrimi	Koha e raportimit	
			Sistem Kritik	Sistem i rëndësishëm
Kategoria 1	<i>Compromised information/</i> Kompromentimi i informacioneve sensitive	<ul style="list-style-type: none">• Ndryshim ose zbulim i informacioneve sensitive• Sulm ndaj informacioneve që	<ul style="list-style-type: none">• Brenda 4 ore nga zbulimi.	<ul style="list-style-type: none">• Brenda 24 orësh nga zbulimi.

Rregullore për Kategoritë e Incidenteve Kibernetike si dhe formatin e elementët e raportit

		konsiderohen pronë intelektuale.		
Kategoria 2	<i>Compromised Asset/</i> Kompromentimi i pajisjeve	<ul style="list-style-type: none"> • Host i komprometuar (root, Trojan, rootkit), • pajisje rrjeti, aplikacione dhe llogari përdoruesi të kompromentuara. • Hoste të infektuara me malware ku sulmuesi kontrollon në mënyrë aktive hostin. 	<ul style="list-style-type: none"> • Brenda 4 ore nga zbulimi. 	<ul style="list-style-type: none"> • Brenda 24 ore nga zbulimi.
Kategoria 3	<i>Unauthorised Access/</i> Akses i paautorizuar	<ul style="list-style-type: none"> • Një individ (i brendshëm apo i jashtëm) ka akses logjik apo fizik pa leje: <ul style="list-style-type: none"> - në një rrjet kombëtar ose lokal - në një sistem - në një aplikacion - tek të dhënat - ose burime të tjera në mënyrë të paautorizuar 	<ul style="list-style-type: none"> • Brenda 4 ore nga zbulimi. 	<ul style="list-style-type: none"> • Brenda 24 orësh nga zbulimi.
Kategoria 4	<i>Malicious Code/</i> Kod keqdashës	<ul style="list-style-type: none"> • Instalim i suksesshëm i software me qëllim të keq si : <ul style="list-style-type: none"> - virus, - worm, - Trojan horse, - ose kode të tjera keqdashëse, <p>që infektojnë një sistem operativ ose aplikacion.</p>	<ul style="list-style-type: none"> • Brenda 4 ore nga zbulimi nëse është shpërndarë në gjithë institucionin. • Brenda 4 dite nga zbulimi nëse nuk është 	<ul style="list-style-type: none"> • Brenda 24 orësh nga zbulimi nëse është shpërndarë në gjithë institucionin. • Brenda 24 dite nga zbulimi nëse nuk është

Rregullore për Kategoritë e Incidenteve Kibernetike si dhe formatin e elementët e raportit

		<ul style="list-style-type: none"> • Institucionet nuk është e nevojshme të raportojnë <i>kode keqdashës</i> që janë detektuar dhe izoluar nga antivirusi. 	shpërndarë.	shpërndarë.
Kategoria 5	<i>Intrusions against networks</i>	<ul style="list-style-type: none"> • Sulm që dëmton funksionalitetin normal të: <ul style="list-style-type: none"> - rrjetave - sistemeve - aplikacioneve, duke shteruar burimet nëpërmjet: <ul style="list-style-type: none"> - DDoS - Web defacement - Sulme brute force, 	<ul style="list-style-type: none"> • Brenda 4 orëve nga zbulimi nëse sulmi është duke vazhduar dhe institucioni nuk është në gjendje ta ndalojë atë. 	<ul style="list-style-type: none"> • Brenda 24 orësh nga zbulimi nëse sulmi është duke vazhduar dhe institucioni nuk është në gjendje ta ndalojë atë.
Kategoria 6	<i>Phishing or Social Engineering</i>	<ul style="list-style-type: none"> • Përdorimi i teknologjisë për të mësuar nga punonjësit e institucionit informacione të rëndësishme si: <ul style="list-style-type: none"> • username • fjalëkalime • informacione të tjera sensitive etj. 	<ul style="list-style-type: none"> • Brenda 4 orësh nga zbulimi. 	<ul style="list-style-type: none"> • Brenda 24 dite nga zbulimi.
Kategoria 7	<i>Unlawful activity / Mashtrimet kompjuterike</i>	<ul style="list-style-type: none"> • Mashtrimet kompjuterike • Pornografia me të mitur • Incidente kompjuterike me natyrë kriminale, zgjidhja e të cilave mund të përfshijë 	<ul style="list-style-type: none"> • Brenda 4 orësh nga zbulimi. 	<ul style="list-style-type: none"> • Brenda 24 dite nga zbulimi.

Rregullore për Kategoritë e Incidenteve Kibernetike si dhe formatin e elementët e raportit

		organe të tjera ligjzbatuese, hetime globale etj.		
Kategoria 8	<i>Scans/Probes/ Attempted Access</i>	<ul style="list-style-type: none"> • Kjo kategori përfshin çdo aktivitet që akseson ose identifikon: <ul style="list-style-type: none"> - një kompjuter të institucionit, - porta të hapura, - protokolle, - shërbime, <p>ose çdo kombinim për ta shfrytëzuar më vonë.</p> <ul style="list-style-type: none"> • Ky aktivitet rezulton direkt në një kompromentim apo mohim të shërbimit. 	<ul style="list-style-type: none"> • Brenda 4 ore nga zbulimi. 	<ul style="list-style-type: none"> • Brenda 24 javësh nga zbulimi.
Kategoria 9	<i>Policy Violations/ Shkelje e politikave të sigurisë së informacionit</i>	<ul style="list-style-type: none"> • Shkelje të qëllimshme të politikave të tilla si: <ul style="list-style-type: none"> - Përdorimi i papërshtatshëm i asetëve të institucionit të tilla si kompjuter, rrjet, ose aplikacion. - Përshkallëzim i paautorizuar i privilegjeve ose përpjekje e qëllimshme për të prishur kontrollet e aksesit. 	<ul style="list-style-type: none"> • Brenda 4 orësh nga zbulimi. 	<ul style="list-style-type: none"> • Brenda 24 jave nga zbulimi.
Kategoria 10	<i>Theft/loss of assets</i>	Vjedhja ose humbja e informacionit ose pajisjeve që mund të përdoren për të përpunuar ose ruajtur informacione sensitive.	<ul style="list-style-type: none"> • Brenda 4 ore nga zbulimi 	<ul style="list-style-type: none"> • Brenda 24 orësh nga zbulimi

Kategoria 11	<i>Unauthorised release of or disclosure of information</i>	Nxjerrja ose publikimi i informacionit në mënyrë paautorizuar	• Brenda 1 ore nga zbulimi	• Brenda 2 orësh nga zbulimi
---------------------	---	---	----------------------------	------------------------------

Procedura e përshkallëzimit të incidentit kibernetik

Procedura e përshkallëzimit të incidentit kibernetik përcakton hapat që ndiqen nga momenti i raportimit të incidentit nga CSIRT sektorial pranë AKCESK nëpërmjet “Formës së raportimit të incidentit kibernetik”, deri në zgjidhjen apo mbylljen e incidentit.

Palët e përfshira në procedurën e përshkallëzuar duhet të evidentohen në varësi të llojit dhe të rëndësisë së incidentit, duke pasur parasysh infrastrukturën e prekur të informacionit.

Një incident si fillim mund të përfshijë vetëm stafin e brendshëm. Drejtuesit e lartë të operatorit që zotëron infrastrukturën mund të njoftohen në një fazë tjetër të trajtimit të incidentit. Nëse incidenti nuk arrin të zgjidhet, duhet të kërkohet mbështetja e palëve të tjera, të tilla si: kompania që ka mirëmbajtjen e sistemit/rrjetit, AKCESK, dhe nëse vlerësohet se incidenti përbën vepër penale të njoftohet Sektori Kundër Krimin Kibernetik në Policinë e Shtetit. **Në momentin që incidenti raportohet pranë Sektorit Kundër Krimin Kibernetik në Policinë e Shtetit, AKCESK pushon së trajtuari incidentin e raportuar.**

Në çdo rast, pavarësisht sesi zgjidhet incidenti, operatori duhet ta raportojë incidentin pranë AKCESK duke plotësuar “Formën e raportimit të incidentit kibernetik”.

Të dhënat mbi incidentet e raportuara do të mblidhen nga AKCESK në një regjistër elektronik me qëllim:

- a) Marrjen e masave për parandalimin e incidenteve të ngjashme në të ardhmen nëpërmjet analizimit të incidentit.
- b) Evidentimin e incidenteve të ndodhura për mbajtjen e statistikave, të cilat japin një panoramë të përgjithshme të llojit, madhësisë dhe frekuencës së incidenteve kibernetike.

Çdo sistem/rrjet duhet të ketë procedurën e vet të përshkallëzimit dhe pikat e kontaktit të cilat plotësojnë nevojat e tyre specifike operacionale. Mund të njoftohen persona të ndryshëm në faza të ndryshme, në varësi të dëmit të sistemit, ose sensitivitetit të të dhënave të prekura.

Pikat e kontaktit që duhen përfshirë, por duke mos u kufizuar vetëm në to, janë:

- Të brendshëm

Rregullore për Kategoritë e Incidenteve Kibernetike si dhe formatin e elementët e raportit

- a) Stafi mbështetës teknik dhe operacional;
 - b) Përgjegjësi i sistemit dhe/ose eprori;
 - c) Oficeri i sigurisë/CSIRT i operatorit
 - d) Koordinatori për informimin, përgatitjen dhe shpërndarjen nëpër media të informacionit.
- Të jashtëm
 - a) Kompania që mirëmban sistemin, zhvilluesit e programeve, këshilluesit e sigurisë etj;
 - b) Ofruesit e Shërbimit (psh. ofruesit e shërbimit të internetit (ISP), palët kontraktore etj.);
 - c) AKCESK;
 - d) Përfaqësues nga Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (IDP);
 - e) Përfaqësues nga Sektori kundër Krimit Kibernetik pranë Policisë së Shtetit;
 - f) Subjektet dhe individët e prekur

Forma e raportimit të incidentit kibernetik			
Seksioni 1: Të dhëna e kontaktit të raportuesit			
Emër Mbiemër:		Pozicioni i punës:	
Institucioni:		E-mail:	
Tel:		Cel:	
Të dhënat e infrastrukturës së prekur nga sulmi			
Emri i sistemit/rrjetit:			
Lloji i infrastrukturës së informacionit:			
<input type="checkbox"/> Kritike			
<input type="checkbox"/> E rëndësishme			
Lloji i asistencës që kërkoni nga AKCESK			
<input type="checkbox"/> Vetëm raportim			
<input type="checkbox"/> Trajtim			
<input type="checkbox"/> Rekomandime			
Seksioni 2 : Detajet e incidentit			
Identifikimi i incidentit			
<input type="checkbox"/> Alarm i pajisjes			
<input type="checkbox"/> Analiza e log-eve			
<input type="checkbox"/> Help Desk			
<input type="checkbox"/> Njoftim nga përdoruesi			
<input type="checkbox"/> Njoftim nga Endpoint Security Software			
<input type="checkbox"/> Tjetër: _____			
Statusi aktual i incidentit			
<input type="checkbox"/> Po ndodh			
<input type="checkbox"/> Nën kontroll			
<input type="checkbox"/> Ka ndodhur			
Kategoria e incidentit			
<input type="checkbox"/> Compromised information			
<input type="checkbox"/> Compromised asset			
<input type="checkbox"/> Unauthorised access			
<input type="checkbox"/> Malicious Code			
<input type="checkbox"/> Intrusions against networks			
<input type="checkbox"/> Theft or Loss			
<input type="checkbox"/> Scans / Probes / Attempted Access			
<input type="checkbox"/> Phishing or Social Engineering			
<input type="checkbox"/> Policy violations			
<input type="checkbox"/> Theft/loss of assets			
<input type="checkbox"/> Unauthorised release of or disclosure of information			
<input type="checkbox"/> Tjetër			
Të dhënat e incidentit			

Rregullore për Kategoritë e Incidenteve Kibernetike si dhe formatin e elementët e raportit

Burimi IP/Port:		Destinacioni IP/Port:	
Të dhënat e përfshira në incident a ishin të enkriptuara:	<input type="checkbox"/> Po	<input type="checkbox"/> Jo	
Kohëzgjatja e incidentit			
Nga data/ora:		Në datën/orën:	
Impakti i incidentit			
Numri i përdoruesve të prekur:			
Koha që sistemi është jashtë shërbimit:			
Dëmi i sistemit:			
Humbja financiare:			
Ka apo jo humbje të dhënash:			
Ju lutem përfshini 5-10 rreshta të “time-stamped logs” në “plain ASCII			
Ju lutem bëni një përshkrim të shkurtër të incidentit dhe pasojave			

Formulari i raportimit të incidentit kibernetik duhet të dërgohet në adresën e e-mailit info@cesk.gov.al.

Incidente që nuk janë të nevojshme të raportohen

- Një malware ose virus në pajisjen e një punonësi që mund të riparohet lehtësisht, psh:
(rast i vetëm i një pajisjeje përdoruesi me një virus që zbulohet automatikisht dhe pastrohet lehtësisht)
- Ndërprerje afatshkurtra në shërbimet jo kritike, psh:
(pajisje që ka një ndërprerje të paplanifikuar e cila është rikthyer lehtësisht në një kohë të shkurtër)
- Raste të vetme të e-maileve standarde të spam-it, te cilat nuk përmbajnë linqe dashakeqe ose dokument bashkangjitur, psh:
(marketing ose reklamë por jo linqe ku mund të klikosh apo dokument bashkangjitur)
- Punonjësit që shkelin politikat ose udhëzimet specifike të institucionit për përdorimin e internetit, psh:
(përdorues të vetëm duke shfletuar faqe të papërshtatshme, por jo të paligjshme ose me qëllim të keq, gjatë kohës së punës)
- Dobësi e shfrytëzuar në sistemet, shërbimet ose rrjetet jo-kritike të informacionit, psh:
(dobësi në desktop –in e një përdoruesi e cila nuk është shfrytëzuar)