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

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	*Compromised information*/ Kompromentimi i informacioneve sensitive	• Ndryshim ose zbulim i informacioneve sensitive • Sulm ndaj informacioneve që	• Brenda 4 ore nga zbulimi.	• Brenda 24 orësh nga zbulimi.

		konsiderohen pronë intelektuale.		
Kategoria 2	*Compromised Asset/* Kompromentimi i pajisjeve	• 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.	• Brenda 4 ore nga zbulimi.	• Brenda 24 ore nga zbulimi.
Kategoria 3	*Unauthorised Access/* Akses i paautorizuar	• Një individ (i brendshëm apo i jashtëm) ka akses logjik apo fizik pa leje: - në një rrjet kombëtar ose lokal - në një sistem - në një aplikacion - tek të dhënat - ose burime të tjera në mënyrë të paautorizuar	• Brenda 4 ore nga zbulimi.	• Brenda 24 orësh nga zbulimi.
Kategoria 4	*Malicious Code/* Kod keqdashës	• Instalim i suksesshëm i software me qëllim të keq si : - virus, - worm, - Trojan horse, - ose kode të tjera keqdashëse, që infektojnë një sistem operativ ose aplikacion.	• Brenda 4 ore nga zbulimi nëse është shpërndarë në gjithë institucionin. • Brenda 4 dite nga zbulimi nëse nuk është	• Brenda 24 orësh nga zbulimi nëse është shpërndarë në gjithë institucionin. • Brenda 24 dite nga zbulimi nëse nuk është

		• Institucionet nuk është e nevojshme të raportojnë *kode keqdashës* që janë detektuar dhe izoluar nga antivirusi.	shpërndarë.	shpërndarë.
Kategoria 5	*Intrusions against networks*	• Sulm që dëmton funksionalitetin normal të: - rrjetave - sistemeve - aplikacioneve, duke shteruar burimet nëpërmjet: - DDoS - Web defacement - Sulme brute force,	• Brenda 4 orëve nga zbulimi nëse sulmi është duke vazhduar dhe institucioni nuk është në gjendje ta ndalojë atë.	• Brenda 24 orësh nga zbulimi nëse sulmi është duke vazhduar dhe institucioni nuk është në gjendje ta ndalojë atë.
Kategoria 6	*Phishing or Social Engineering*	• Përdorimi i teknologjisë për të mësuar nga punonjësit e institucionit informacione të rëndësishme si: • username • fjalëkalime • informacione të tjera sensitive etj.	• Brenda 4 orësh nga zbulimi.	• Brenda 24 dite nga zbulimi.
Kategoria 7	*Unlawful activity / Mashtrimet kompjuterike*	• Mashtrimet kompjuterike • Pornografia me të mitur • Incidente kompjuterike me natyrë kriminale, zgjidhja e të cilave mund të përfshijë	• Brenda 4 orësh nga zbulimi.	• Brenda 24 dite nga zbulimi.

		organe të tjera ligjzbatuese, hetime globale etj.		
Kategoria 8	*Scans/Probes/ Attempted Access*	• Kjo kategori përfshin çdo aktivitet që akseson ose identifikon: - një kompjuter të institucionit, - porta të hapura, - protokolle, - shërbime, ose çdo kombinim për ta shfrytëzuar më vonë. • Ky aktivitet rezulton direkt në një kompromentim apo mohim të shërbimit.	• Brenda 4 ore nga zbulimi.	• Brenda 24 javësh nga zbulimi.
Kategoria 9	*Policy Violations/ Shkelje e politikave të sigurisë së informacionit*	• Shkelje të qëllimshme të politikave të tilla si: - Përdorimi i papërshtatshëm i aseteve të institucionit të tilla si kompjuter, rrjet, ose aplikacion. - Përshkallëzim i paautorizuar i privilegjeve ose përpjekje e qëllimshme për të prishur kontrollet e aksesit.	• Brenda 4 orësh nga zbulimi.	• Brenda 24 jave nga zbulimi.
Kategoria 10	*Theft/loss of assets*	Vjedhja ose humbja e informacionit ose pajisjeve që mund të përdoren për të përpunuar ose ruajtur informacione sensitive.	• Brenda 4 ore nga zbulimi	• Brenda 24 orësh nga zbulimi

Kategoria 11	*Unauthorised release of or disclosure of information*	Nxjerrja ose publikimi i informacionit në mënyrë të 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 Krimit Kibernetik në Policinë e Shtetit. **Në momentin që incidenti raportohet pranë Sektorit Kundër Krimit 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

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: ☐ Kritike			
☐ E rëndësishme			
Lloji i asistencës që kërkoni nga AKCESK			
☐ Vetëm raportim	☐ Trajtim	☐ Rekomandime	
Seksioni 2 : Detajet e incidentit			
Identifikimi i incidentit			
☐ Alarm i pajisjes	☐ Analiza e log-eve	☐ Help Desk	
☐ Njoftim nga përdoruesi	☐ Njoftim nga Endpoint Security Software		
☐ Tjetër: _____			
Statusi aktual i incidentit			
☐ Po ndodh	☐ Nën kontroll	☐ Ka ndodhur	
Kategoria e incidentit			
☐ Compromised information	☐ Compromised asset	☐ Unauthorised access	☐ Malicious Code
☐ Intrusions against networks	☐ Theft or Loss	☐ Scans / Probes / Attempted Access	
☐ Phishing or Social Engineering	☐ Policy violations	☐ Theft/loss of assets	
☐ Unauthorised release of or disclosure of information	☐ Tjetër		
Të dhënat e incidentit			

Burimi IP/Port:		Destinacioni IP/Port:	
Të dhënat e përfshira në incident a ishin të enkriptuara:	☐ Po	☐ 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*)