REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 713 Prot. Tiranë më, 21 . 08 . 2024

U R DH Ë R
Nr. 299, datë 21 / 08 / 2024

PËR
MIRATIMIN E RREGULLORES "PËR KATEGORIZIMIN E INCIDENTEVE TË SIGURISË KIBERNETIKE"

Në zbatim të pikës 8 të nenit 23, të ligjit nr. 25/2024 "Për sigurinë kibernetike",

U R DH Ë R O J:

1. Miratimin e rregullores "Për kategorizimin e 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, CSIRT-et pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe subjektet e tjera të cilat bëjnë njoftimin vullnetar të incidentit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTOR I PËRGJITHSHËM

Igli TAFA

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

RREGULLORE

PËR KATEGORIZIMIN E INCIDENTEVE TË SIGURISË KIBERNETIKE

PËRMBAJTJA **faqe**

Hyrje.....3

KREU I: DISPOZITA TË PËRGJITHSHME.....3

Qëllimi.....3

Baza ligjore.....3

Fusha e zbatimit.....3

Përkufizime.....4

KREU II: KATEGORIZIMI I INCIDENTEVE TË SIGURISË KIBERNETIKE.....5

Llojet e incidenteve kibernetike.....5

Kategoritë e incidenteve kibernetike.....6

Prioritizimi i incidentit.....9

KREU III: RAPORTIMI I INCIDENTEVE TË SIGURISË KIBERNETIKE.....11

Raportimi i incidenteve kibernetike dhe forma e raportimit.....13

Procedura e raportimit të incidentit të sigurisë kibernetike.....13

Njoftimi vullnetar i incidentit dhe procedura e raportimit.....13

KREU IV: DOKUMENTIMI I INCIDENTEVE TË SIGURISË KIBERNETIKE.....14

Dokumentimi i incidentit të sigurisë kibernetike.....14

Regjistri i incidenteve të sigurisë kibernetike.....14

TABELAT.....

Tabela 1 Llojet e incidenteve të sigurisë kibernetike.....5

Tabela 2: Kategorizimi i incidenteve bazuar në skemën e ENISA-s.....6

Tabela 3: Prioritizimi i Incidenteve dhe Task forca e reagimit sipas impaktit të incidentit.....
10

ANEKSET.....15

Aneksi I Formati i Raportimit të incidentit brenda 4 orësh.....15

Aneksi II Formati i Raportimit të incidentit brenda 72 orësh.....17

Aneksi III Formati i regjistrit të incidentit nga operatorët e infrastrukturave kritike dhe të rëndësishme..... 18

Aneksi IV Formati i regjistrit të incidenteve kibernetike që administrohet nga Autoriteti Kombëtar për Sigurinë Kibernetike.....19

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 dhe elementëve të raportimit të incidentit të sigurisë kibernetike.

KREU I

DISPOZITA TË PËRGJITHSHME

Neni 1
Qëllimi

Qëllimi i hartimit të kësaj rregulloreje është përcaktimi i llojeve dhe kategorive të incidenteve të sigurisë kibernetike, të cilat prekin sistemet dhe rrjetet e informacionit, formatin, elementet e raportimit, afatet e raportimit, mënyrën e dokumentimit dhe të regjistrimit të incidenteve kibernetike.

Neni 2
Baza ligjore

Kjo rregullore është hartuar në zbatim nenit 9 shkronja “g”, nenit 17, pika 3 shkronja “b”, “c” dhe “d” nenit 23, pika 3, 4, 5, 6, 8, nenit 25 të ligjit nr. 25/2024 “Për sigurinë kibernetike”.

Neni 3
Fusha e zbatimit dhe subjektet përgjegjës

Përcaktimet e kësaj rregulloreje zbatohen nga CSIRT-it Kombëtar, dhe CSIRT-it pranë operatorit për të klasifikuar, prioritizuar, raportuar, dokumentuar dhe regjistruar incidentin kibernetik. Gjithashtu, kjo rregullore zbatohet edhe nga subjektet e tjera të cilat bëjnë njoftimin vullnetar të incidentit.

Neni 4
Përkufizime

Në kuptim të kësaj rregulloreje, termat e mëposhtëm kanë këto kuptime:

1. **"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.
2. **"Incident kibernetik i rëndësishëm"**, është një incident i cili:
a) ka shkaktuar ose është në gjendje të shkaktojë ndërprerje të rëndë operacionale të shërbimeve ose humbje financiare për operatorin e prekur ;
b) ka ndikuar ose është në gjendje të prekë persona të tjerë fizikë ose juridikë duke shkaktuar dëme të konsiderueshme materiale ose jo materiale.
3.**"Infrastrukturë kritike e informacionit"**, është tërësia e rrjeteve dhe sistemeve të informacionit, të zotëruara nga një autoritet publik ose privat, që ofrojnë shërbime, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
4. **"Infrastrukturë e rëndësishme e informacionit"**, është tërësia e rrjeteve dhe sistemeve të informacionit të zotëruara nga një autoritet publik ose privat, i cili nuk është pjesë e infrastrukturës kritike të informacionit, por që mund të rrezikojë apo të kufizojë ofrimin e shërbimit dhe vazhdimësinë e punës, në rastin e cenimit të sigurisë së informacionit.
5. **"Kërcënim kibernetik**", është një ngjarje ose veprim i mundshëm që mund të dëmtojë, ndërpresë ose ndikojë negativisht në rrjetet dhe sistemet e informacionit, për përdoruesit e tyre dhe persona të tjerë.
6. "Operator i infrastrukturës kritike të informacionit", është çdo person fizik ose juridik i cili administron infrastrukturën kritike të informacionit dhe plotëson kërkesat e përcaktuara në këtë ligj.
7. **"Operator i infrastrukturës së rëndësishme të informacionit"**, është çdo person fizik ose juridik, i cili administron infrastrukturën e rëndësishme të informacionit dhe plotëson kërkesat e përcaktuara në këtë ligj
8**. "Rrezik i sigurisë kibernetike"**, është një ngjarje, e identifikueshme me efekt të mundshëm negativ për sigurinë e rrjeteve dhe sistemeve të informacionit.
9. **"Trajtimi i incidentit të sigurisë kibernetike"**, janë të gjitha procedurat e nevojshme për parandalimin, identifikimin, analizimin, reagimin dhe rikuperimin ndaj një incidenti të sigurisë kibernetike.
10. "Vulnerabilitet" është një dobësi, ndjeshmëri ose defekt i produkteve ose shërbimeve TIK që mund të shfrytëzohet nga një kërcënim kibernetik.

KREU II

KATEGORIZIMI DHE LLOJET E INCIDENTEVE TË SIGURISË KIBERNETIKE

Neni 5

Llojet e incidenteve të sigurisë kibernetike kibernetike

1. Kjo rregullore përcakton 3 (tre) lloje të incidenteve të sigurisë kibernetike, siç detajohet në tabelën *1* të kësaj rregulloreje.

2. Llojet e incidenteve të sigurisë kibernetike janë si vijojnë:

a) b) incidente kibernetike me ndikim të lartë;
b) incidente kibernetike me ndikim mesatar;
c) ç) incidente kibernetike me ndikim minimal;

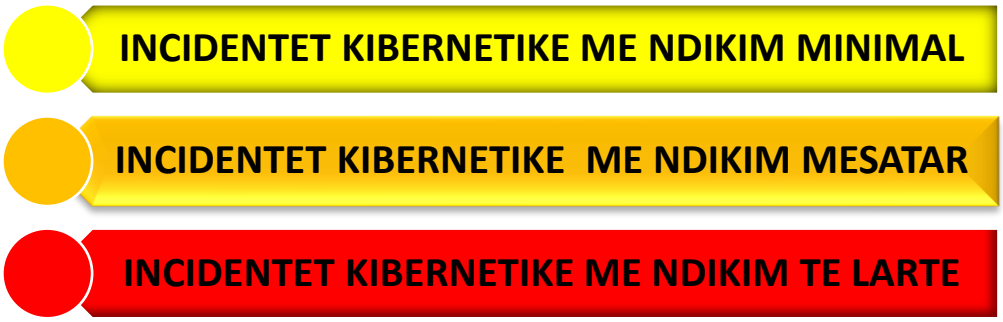
3. Incidente kibernetike me ndikim të lartë janë incidente kibernetike të rëndë me ndikim të lartë në operacionet e rëndësishme ose të dhënat e ndjeshme. Këto incidente kërkojnë mobilizimin e shpejtë të ekipeve të përgjigjes ndaj incidenteve dhe mund të përfshijnë informimin e palëve të interesuara dhe autoriteteve rregullatorë.

4. Incidente kibernetike me ndikim mesatar janë incidente kibernetike me ndikim mesatar që mund të kenë pasoja të kufizuara në integritetin, disponueshmërinë ose konfidencialitetin e sistemeve ose të dhënave. Këto incidente kërkojnë një përgjigje të koordinuar për të adresuar dobësitë dhe për të rivendosur shërbimet normale.

5. Incident me ndikim minimal janë incidente me ndikim të ulët që kryesisht kanë pasoja minimale dhe të menaxhueshme. Këto incidente mund të trajtohen nga procedurat e zakonshme operative pa ndërhyrje të veçantë.

Tabela 1 Llojet e incidenteve të sigurisë kibernetike

Llojet e incidenteve kibernetike	Përshkrim
INCIDENTET KIBERNETIKE ME NDIKIM TË LARTË	Përfaqëson një situatë kritike që prek operacionet kyçe ose të dhënat e ndjeshme, duke shkaktuar ndërprerje të rëndësishme apo rrezik të madh për sigurinë e informacionit. Kjo lloj situate kërkon reagim të menjëhershëm dhe të koordinuar nga ekipet e specializuara, si dhe mund të kërkojë njoftimin e menjëhershëm të palëve të interesuara dhe autoriteteve përkatëse për të minimizuar pasojat e mëtejshme.
INCIDENTET KIBERNETIKE ME NDIKIM MESATAR	Përfaqëson incidente me ndikim mesatar që mund të kenë pasoja të kufizuara në integritetin, disponueshmërinë ose konfidencialitetin e sistemeve ose të dhënave. Kërkon përgjigje të koordinuar për të adresuar dobësitë dhe për të rivendosur shërbimet normale.
INCIDENTET KIBERNETIKE ME NDIKIM MINIMAL	Tregon incidente me ndikim të ulët që kryesisht kanë pasoja minimale dhe të menaxhueshme. Këto incidente mund të trajtohen nga procedurat e zakonshme operative pa ndërhyrje të veçantë.



Legjenda: Shpjegim i tabelës referuar ngjyrave

Neni 6

Kategoritë e incidenteve të sigurisë kibernetike

1. Kategorizimi i incidenteve të sigurisë kibernetike ndihmon për të planifikuar veprimet për trajtimin dhe zgjidhjen e incidentit të sigurisë kibernetike si dhe përcakton formatet e raportimit në varësi të ndikimit të incidentit kibernetik.

2. Kjo rregullore përcakton 12 (dymbëdhjetë) kategori të incidenteve kibernetike siç detajohet në tabelën 2 të kësaj rregulloreje. Kategoritë e incidenteve të sigurisë kibernetike janë si vijojnë:

a) përmbajtje abuzive;

b) kod keqdashës;

c) mbledhja e informacionit;

ç) përpjekjet për ndërhyrje;

d) ndërhyrjet;

e) disponueshmëria;

ë) siguria e përmbajtjes së informacionit;

f) mashtrimi;

g) vulnerabiliteti;

gj) cryptomining;

h) eksfiltrimi;

i) incident në ambjent testimi.

3. Përcaktimi i kategorive të incidenteve kibernetike është bërë bazuar në Klasifikimin e incidenteve të publikuar nga Agjencia e Sigurisë Kibernetike e Bashkimit Evropian (ENISA).

Tabela 2: Kategorizimi i incidenteve

Nr	KATEGORITË E INCIDENTEVE	NËNKATEGORI TË INCIDENTEVE	PËRSHKRIM
1	**Përmbajtje abuzive**	Spam	Dërgimi në grup i postës elektronike pa aprovimin e marrësit, e cila mund të përmbajë malware, ose skema mashtruese me qëllim kompromentimin e sigurisë së informacionit të përdoruesve.
		Të folurit e dëmshëm	Diskreditimi ose diskriminimi i dikujt (p.sh. ndjekja kibernetike, racizmi dhe kërcënimet ndaj një ose më

				shumë individëve).
		Përmbajtje online e dhunshme/seksuale/bullizuese ndaj fëmijëve		Pornografia e fëmijëve, shpërndarja e materialeve të dhunshme etj.
		Keqinformimi me dashje		Shtrembërimi i informacionit, i cili ka për qëllim të shkaktojë panik.
2	**Kod keqdashës**	Virus drejt shërbimeve kritike	Virus drejt shërbimeve të tjera	Software që instalohet qëllimisht në një sistem për qëllime të dëmshme.
		Worm drejt shërbimeve kritike	*Worm* drejt shërbimeve të tjera	
		Trojan drejt shërbimeve kritike	Trojan drejt shërbimeve të tjera	
		Spyware drejt shërbimeve kritike	*Spyware* drejt shërbimeve të tjera	
		Dialler drejt shërbimeve kritike	*Dialler* drejt shërbimeve të tjera	
		Rootkit drejt shërbimeve kritike	*Rootkit* drejt shërbimeve të tjera	
		Ransomware drejt sistemeve kritike	Ransomware drejt sistemeve të tjera	Kod keqdashës, i cili enkripton të dhënat në sistemet kompjuterike të një përdoruesi fundor ose/edhe servera.
		Fshirja e të dhënave *(wiper)* në sistemet kritike	Fshirja e të dhënave *(wiper)* në sistemet e tjera	Kod keqdashës, i cili ka për qëllim të shkatërrojë ose të fshijë të dhënat nga sistemi i prekur, duke bërë që të dhënat të bëhen të papërdorshme ose sistemi të mos funksionojë më.
3	**Mbledhja e informacionit**	Skanimi		Kërkesa për të zbuluar pikat e dobëta të një sistemi. Gjithashtu, kjo kategori incidenti përfshin procesin e testimit, me qëllim mbledhjen e informacioneve rreth hosteve, shërbimeve dhe llogarive. Shembuj: *fingered, DNS Query, RCE, ICMP, SMTP (EXPN, RCPT, etj.),* skanim i portave.
		Sniffing drejt shërbimeve kritike	*Sniffing* drejt shërbimeve të tjera	Vëzhgimi dhe regjistrimi i trafikut të rrjetit (përgjimi).
		Inxhinieria sociale		Mbledhja e informacionit nga përdoruesit fundorë, në mënyrë jo-teknike (p.sh. mashtrime, "shoulder surfing", "*tailgating*", "*piggybacking*", Spiunazh ose kërcënime).
4	**Përpjekjet për ndërhyrje**	Shfrytëzimi i vulnerabiliteteve të njohura për të aksesuar shërbime kritike	Shfrytëzimi i vulnerabiliteteve të njohura për të aksesuar shërbime të tjera.	Përpjekje për të kompromentuar një sistem ose për të ndërprerë shërbime duke shfrytëzuar vulnerabilitetet, p.sh, backdoor, fragmentimi, etj.
		Përpjekjet për *login*		Përpjekje të shumta për login, p.sh, *Guessing / cracking of passwords, dictionary attack, brute force, RCE.*
		0-day attack drejt shërbimeve kritike	0-day attack drejt shërbimeve të tjera	Përpjekje për ndërhyrje duke përdorur një *exploit* të panjohur.
		Kompromentim i llogarive të privilegjuara		Kompromentim i suksesshëm i një sistemi ose

<table>
<tr><td rowspan="2">5</td><td rowspan="2">Ndërhyrjet</td><td colspan="2">Kompromentim i llogarive të paprivilegjuara</td><td>aplikacioni (shërbimi). Ky incident mund të shkaktohet nga nga një vulnerabilitet i njohur ose i ri, por edhe nga aksesi lokal i paautorizuar.</td></tr>
<tr><td>Kompromentim i një aplikacioni që ofron shërbim kritik</td><td>Kompromentim i një aplikacioni që ofron shërbime të tjera</td><td>Psh ekzekutimi i teknikave injection si: SQL Injection, Command Injection, File Injection, XSS, CSRF, RCE, API attack etj.</td></tr>
<tr><td rowspan="6">6</td><td rowspan="6">Disponueshmëria</td><td colspan="2">DoS/DDoS që ka ndërprerë sherbime kritike</td><td rowspan="6">DoS është një taktikë e sulmit kibernetik ku një sistem kompjuterik përdoret për të bombarduar një server, shërbim, ose rrjet me trafik të madh për të shkaktuar mbingarkesë dhe parandaluar përdorimin normal të shërbimit nga përdoruesit legjitimë.

Kur në këtë sulm përfshihen më shumë se një sistem kompjuterik i infektuar, kategorizohet si DDoS. DDoS shpesh bazohet në sulmet DoS me origjinë nga botnet, por ekzistojnë edhe skenarë të tjerë si sulmet e Amplifikimit DNS.

Disa shembuj, janë ICMP flood, SYN, sulmet Teardrop dhe mail-bombing.

Disponueshmëria mund të afektohet edhe nga veprimet lokale (shkatërrim, ndërprerje e furnizimit me energji elektrike, etj.) - ose nga ngjarje katastrofike natyrore, dështime spontane ose gabime njerëzore, pa përfshirë keqdashje ose neglizhencë.</td></tr>
<tr><td colspan="2">DoS/DDoS që ka ndikuar ndjeshëm shërbimet kritike dhe/ose ka ndërprerë shërbimet e tjera</td></tr>
<tr><td colspan="2">DoS/DDoS që nuk ka ndikim në shërbime kritike, por ka ndikuar ndjeshëm tek shërbimet e tjera.</td></tr>
<tr><td>Sabotimi që ka prekur sistemin kritik</td><td>Sabotimi që ka prekur sisteme të tjera.</td></tr>
<tr><td>Ndërprerje e shërbimeve si pasojë e një incidenti gjatë procesit të mirëmbajtjes ose/edhe teknike si: Energjia/Zjarri/Përmbytje që ka prekur infrastrukturën kritike</td><td>Ndërprerje e shërbimeve si pasojë e procesit të mirëmbajtjes ose/edhe teknike si: Energjia/Zjarri/ Përmbytje që ka prekur shërbime të tjera</td></tr>
<tr><td>Ndërprerje për shkak të katastrofave natyrore që ka prekur infrastrukturen kritike</td><td>Ndërprerje për shkak të katastrofave natyrore për shërbime të tjera</td></tr>
<tr><td rowspan="2">7</td><td rowspan="2">Siguria e Përmbajtjes së Informacionit</td><td>Akses i paautorizuar në shërbime kritike</td><td>Akses i paautorizuar në shërbime të tjera</td><td rowspan="2">Siguria e përmbajtjes së informacionit mund të cënohet nga kompromentim i suksesshëm i llogarive, aplikacioneve, të dhënave dhe sistemeve.
Gjithashtu, sulmet mund të përgjojnë dhe aksesojnë informacionin gjatë transmetimit (wiretapping, spoofing or hijacking).

Këto sulme mund të shkaktohen nga gabimet njerëzore, të konfigurimit, ose erore të softuerit.</td></tr>
<tr><td>Modifikimi i paautorizuar në shërbime kritike</td><td>Modifikimi i paautorizuar në shërbime të tjera</td></tr>
<tr><td rowspan="2">8</td><td rowspan="2">Mashtrimi</td><td colspan="2">Përdorimi i paautorizuar i burimeve</td><td>Përdorimi i paautorizuar i burimeve, për qëllime përfitimesh personale të palidhura me aktivitetin e punës, si: chain-letter, përdorimi i emaileve të punës për regjistrimin në platforma që nuk lidhen me aktivititetin e punës, etj.</td></tr>
<tr><td colspan="2">E drejta e autorit</td><td>Ofrimi ose instalimi i kopjeve të softuerit komercial të paliçensuar ose materialeve të tjera të mbrojtura nga e drejta e autorit.</td></tr>
</table>

		Maskimi			Teknikë e sulmit ku një individ ose proces përpiqet të fitojë qasje të paautorizuar në burime ose të dhëna duke u përfaqësuar si një entitet legjitim. Kjo bëhet përmes falsifikimit të identitetit të tyre, si përmes përdorimit të të dhënave të vjedhura për autentifikim ose manipulimit të protokolleve të rrjetit për të mashtruar sistemet e sigurisë që të besojnë se trafiku ose kërkesat janë nga një burim i lejuar.
		Phishing/Spear Phishing/Whaling/Smishing/Vishing			Phishing është një teknikë mashtrimi që synon të marrë informacione të ndjeshme përmes email-eve, mesazheve, telefonatave, të targetuara (*spear phishing*), për nivelet e larta drejtuese (whaling), ose të pa targetuara, dërguesi i të cilave pretendon të jetë një entitet legjitim.
9	**Dobesi (Vulnerabiliteti)**	Vulnerabilitete të dukshme për abuzim në shërbime kritike	Vulnerabilitete të dukshme për abuzim në shërbime të rëndësishme	Vulnerabilitete të dukshme për abuzim në shërbime të tjera	Vulnerabilitete të cilat bëhen publike nga palë të paautorizuara dhe i përkasin shërbimeve të një infrastrukture informacioni.
10	**Cryptomining**	Cryptomining në sistemet kritike ose në sisteme të tjera			Shfrytëzimi i burimeve për qëllime përfitimi nga gjenerimi i monedhave virtuale, si psh: Bitcoin.
11	**Eksfiltrimi**	Nxjerrja e të dhënave nga sistemet kritike të infrastrukturës drejt një serveri C2	Nxjerrja e të dhënave nga sistemet e tjera të infrastrukturës drejt një serveri C2		Procesi i paautorizuar i nxjerrjes së të dhënave nga sistemet e infrastrukturës drejt një serveri C2 për qëllime keqdashëse.
12	**Incident në ambjent testimi**	Incident i ndodhur në ambjent testimi për sistemet kritike ose sistemet e tjera			Keqpërdorimi i të dhënave sensitive në ambjent testimi si psh: Në sistemin financiar kur implementohet një sistem i ri dhe përdoren të dhënat reale të klientëve duhet të shfrytëzohet standarti PCI DSS → Marrjen leje të dhënave, dhe në fund shkatërrimin e tyre në mënyrë të përhershme.

Neni 7

Prioritizimi i Incidentit

1. Bazuar në llojet dhe kategoritë e incidentit kibernetik të ndodhur dhe impaktin e tij, ekipet e përgjigjes së incidentit pranë operatorit dhe në Autoritetin Kombëtar të Sigurisë Kibernetike bëjnë prioritizimin e incidentit kibernetik.
2. Prioritizimi i incidentit parashikon tre (tre) klasifikime dhe në varësi të prioritizimit përcaktohet task forca, e cila do të ndërmarrë masat për të reaguar ndaj incidentin si dhe për të analizuar incidentin si në tabelën më poshtë:

Tabela 1: Prioritizimi i Incidenteve dhe Task forca e reagimit sipas impaktit të incidentit

Klasifikimi i incidenteve	Përshkrim	Task Forca e Analizës dhe Reagimit
INCIDENTET ME NDIKIM TË LARTË	Tregon një incident të rëndë me ndikim të lartë në operacionet e rëndësishme ose të dhënat e ndjeshme. Kërkon mobilizimin e shpejtë të ekipeve të përgjigjes ndaj incidenteve dhe mund të përfshijë informimin e palëve të interesuara dhe autoriteteve rregullatore.	Një minimum prej **6 ekspertësh**, duke përfshirë të paktën një ekspert në monitorimin dhe reagimin ndaj incidenteve kibernetike, një ekspert në mbrojtjen dhe menaxhimin e incidenteve, një ekspert në simulimet e incidenteve kibernetike, një ekspert në hetimin e incidenteve kibernetike, si dhe përfaqësues nga departamentet e infrastrukturës së prekur dhe përfaqësues nga departamentet e infrastrukturës së prekur. Ky ekip koordinohet me Policinë e Shtetit dhe institucionet përkatëse ligjzbatuese. Në këtë operacion mund të përfshihen organizatat partnere kombëtare ose ndërkombëtare. Pjesë e komunikimit dhe bashkërendimit të punës mund të bëhet me propozimin e Drejtorit të Përgjithshëm edhe CERT-i Kombëtar.
INCIDENTE ME NDIKIM MESATAR	Përfaqëson incidente me ndikim mesatar që mund të kenë pasoja të kufizuara në integritetin, disponueshmërinë ose konfidencialitetin e sistemeve ose të dhënave. Kërkon përgjigje të koordinuar për të adresuar dobësitë dhe për të rivendosur shërbimet normale.	Të paktën **4 ekspertë** në gatishmëri, duke përfshirë specialistë në rikuperimin e sistemit, sigurinë e rrjetit dhe mbrojtjen e të dhënave. Ky ekip koordinohet me Policinë e Shtetit dhe institucionet përkatëse ligjzbatuese.
INCIDENTET ME NDIKIM MINIMAL	Tregon incidente me ndikim të ulët që kryesisht kanë pasoja minimale dhe të menaxhueshme. Këto incidente mund të trajtohen	Të paktën **2 ekspertë** në gatishmëri për të vlerësuar dhe zbutur incidentin. Ky ekip koordinohet me Policinë e Shtetit dhe institucionet përkatëse ligjzbatuese.

	nga procedurat e zakonshme operative pa ndërhyrje të veçantë.	

KREU III

RAPORTIMI I INCIDENTEVE TË SIGURISË KIBERNETIKE

Neni 8
Raportimi i incidentit të sigurisë kibernetike

1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, kanë detyrimin të raportojnë pranë CSIRT-it kombëtar dhe CSIRT-it sektorial, të gjitha kategoritë e incidenteve të sigurisë kibernetike sipas nenit 6, pika 2 detajuar në tabelën nr.2, brenda 4 orëve, nga momenti i identifikimit të incidentit si dhe të vendosin në dispozicion kopjen e logeve.
2. Në rastin e incidenteve të rëndësishme, operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin që brenda 72 orëve nga momenti i identifikimit të të përditësojnë informacionin dhe të bëjnë një vlerësim fillestar të incidentit të rëndësishëm, duke përfshirë ashpërsinë, ndikimin, si dhe, aty ku ka, treguesit e kompromentimit. Referuar kategorive dhe nënkategorive të incidenteve të përcaktuar ne nenin 6, pika 2 dhe të detajuar në tabelën 2 të kësaj rregulloreje, konsiderohen incidente të rëndësishme, kategoritë 1-11 si dhe të gjitha nënkategoritë e incidenteve me ndikim të lartë dhe mesatar konkretisht si vijon:

a. Përmbajtje online e dhunshme/seksuale/bullizuese ndaj fëmijëve;
b. Keqinformimi me dashje;
c. Virus drejt shërbimeve kritike/ Virus drejt shërbimeve të tjera;
d. *Worm* drejt shërbimeve kritike/ *Worm* drejt shërbimeve të tjera;
e. Trojan drejt shërbimeve kritike/ Trojan drejt shërbimeve të tjera;
f. *Spyware* drejt shërbimeve kritike/ *Spyware* drejt shërbimeve të tjera;
g. *Dialler* drejt shërbimeve kritike/ *Dialler* drejt shërbimeve të tjera;
h. *Rootkit* drejt shërbimeve kritike/ *Rootkit* drejt shërbimeve të tjera;
i. Ransomware drejt sistemeve kritike/ Ransomware drejt sistemeve të tjera;
j. Fshirja e të dhënave *(wiper)* në sistemet kritike/ Fshirja e të dhënave *(wiper)* në sistemet e tjera;
k. *Sniffing* drejt shërbimeve kritike;
l. Shfrytëzimi i vulnerabiliteteve të njohura për të aksesuar shërbime kritike /Shfrytëzimi i vulnerabiliteteve të njohura për të aksesuar shërbime të tjera;
m. Përpjekjet për *login;*
n. *0-day attack* drejt shërbimeve kritike/*0-day attack* drejt shërbimeve të tjera;
o. Kompromentim i llogarive të privilegjuara/ Kompromentim i llogarive të paprivilegjuara;

p. Kompromentim i një aplikacioni që ofron shërbim kritik/ Kompromentim i një aplikacioni që ofron shërbime të tjera;
q. DoS/DDoS që ka ndërprerë sherbime kritike/ DoS/DDoS që ka ndikuar ndjeshëm shërbimet kritike dhe/ose ka ndërprerë shërbimet e tjera;
r. Sabotimi që ka prekur sistemin kritik;
s. Ndërprerje e shërbimeve si pasojë e një incidenti gjatë procesit të mirëmbajtjes ose/edhe teknike si: Energjia/Zjarri/Përmbytje që ka prekur infrastrukturën kritike;
t. Ndërprerje për shkak të katastrofave natyrore që ka prekur infrastrukturen kritike;
u. Akses i paautorizuar në shërbime kritike/ Akses i paautorizuar në shërbime të tjera;
v. Modifikimi i paautorizuar në shërbime kritike/ Modifikimi i paautorizuar në shërbime të tjera;
w. Përdorimi i paautorizuar i burimeve;
x. Vulnerabilitete të dukshme për abuzim në shërbime kritike/ Vulnerabilitete të dukshme për abuzim në shërbime të rëndësishme;
y. Cryptomining në sistemet kritike ose në sisteme të tjera;
z. Nxjerrja e të dhënave nga sistemet kritike të infrastrukturës drejt një serveri C2/ Nxjerrja e të dhënave nga sistemet e tjera të infrastrukturës drejt një serveri C2;

3. Raportimi sipas pikës 1 dhe 2 të këtij neni do të bëhet në përputhje me formatin në aneksin 1 dhe 2 bashkëlidhur kësaj rregulloreje.

4. Për të përcaktuar rëndësinë e ndikimit të një incidenti kibernetik, vlerësohen parametrat e mëposhtëm:

a) numri i përdoruesve të prekur nga ndërprerja e shërbimit;

b) kohëzgjatja e incidentit;

c) shtrirja gjeografike në lidhje me zonën e prekur nga incidenti;

ç) shkalla e ndërprerjes së funksionimit të shërbimit;

d) shtrirja e ndikimit në aktivitetet ekonomike dhe shoqërore;

dh) varësia e sektorëve nga shërbimet e ofruara të operatorit të infrastrukturës së informacionit;

e) rëndësia e ruajtjes së një niveli të mjaftueshëm të shërbimit, duke marrë parasysh disponueshmërinë e mjeteve alternative për sigurimin e këtij shërbimi.

5. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit brenda një muaj pas njoftimit të incidentit sipas pikës 1 dhe 2 të këtij neni duhet t' i dorëzojnë CSIRT-it kombëtar një raport përfundimtar, i cili përmban:

i. një përshkrim të detajuar të incidentit, duke përfshirë rëndësinë dhe ndikimin e tij;

ii. llojin e kërcënimit ose shkakun kryesor që mund ta ketë shkaktuar incidentin;

iii. masat e aplikuara dhe masat e vazhdueshme për zvogëlimin e pasojave;

iv. aty ku është e aplikueshme, ndikimin ndërkufitar të incidentit.

6. Në rastet e një incidenti kibernetik të vazhdueshëm operatori i infrastrukturës së informacionit i prekur nga ky incident përveç detyrimit të dorëzimit të raportit përfundimtar në kohën e mbylljes së incidentit kibernetik sipas pikës 5 të këtij neni, ka detyrimin të dorëzojë pranë CSIRT-it Kombëtar edhe një raport progresi.

Neni 9
Procedura e raportimit të incidentit kibernetik

Në rastin e një incidenti të sigurisë kibernetike, pika e kontaktit të infrastrukturës së informacionit në të cilën ka ndodhur incidenti, raporton incidentin kibernetik pranë CSIRT-it Kombëtar nëpërmjet:
a) platformës së raportimit,
b) shkresës zyrtare,
c) email-it.
d) telefonit, numri i dedikuar pranë CSIRT-it Kombëtar.

Neni 10
Njoftimi vullnetar i incidentit

1. Përveç operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit raportojnë vullnetarisht pranë CSIRT-it kombëtar, incidentet kibernetike edhe subjektet e tjera.
2. Raportimi vullnetar nuk krijon pasoja apo detyrime për subjektin raportues, nëse ai nuk do të kishte bërë një raportim të tillë.
3. Subjektet e tjera raportojnë incidentin kibernetik sipas përcaktimeve të nenit 8 të kësaj rregulloreje si dhe sipas formateve të raportimit të përcaktuara ne Aneksin 1, Aneksin 2 të kësaj rregulloreje si dhe Raportin sipas pikës 5 të nenit 8 të kësaj rregulloreje.
4. Procedura e raportimit të incidentit kibernetik nga subjektete e tjera kryhet nëpërmjet:
   a) shkresës zyrtare,
   b) email-it.
   c) telefonit, numri i dedikuar pran CSIRT-it Kombëtar.

Neni 11
Incidente të cilat nuk raportohen

Nuk ka nevojë të raportohen incidentet kibernetike si më poshtë vijon:

a. Një malware ose virus në pajisjen e një punonjësi që mund të riparohet lehtësisht, p.sh.: (rast i vetëm i një pajisjeje përdoruesi me një virus që zbulohet automatikisht dhe pastrohet lehtësisht)
b. Ndërprerje afatshkurtra në shërbime jo kritike, p.sh.: (pajisje që ka një ndërprerje të paplanifikuar e cila u rikthye lehtësisht në një kohë të shkurtër)
c. Punonjësit që shkelin politikat ose udhëzimet specifike të institucionit për përdorimin e internetit, p.sh.: (përdorues të vetëm që shfletojnë faqe të papërshtatshme, por jo të paligjshme ose keqdashëse, gjatë orëve të punës)
d. Dobësi të pashfrytëzuara në sisteme, shërbime ose rrjete jo kritike të informacionit, p.sh.: (dobësi në desktopin e një përdoruesi që nuk është shfrytëzuar)

KREU IV

DOKUMENTIMI I INCIDENTEVE TË SIGURISË KIBERNETIKE

Neni 12
Dokumentimi dhe regjistrimi i incidentit nga operatorët e infrastrukturës kritike

1. Operatorët e infrastrukturave kritike dhe të rëndësishme dokumentojnë të gjithë informacionin e rëndësishëm dhe kronologjinë e incidentit.
2. Dokumentimi i incidentit konsiderohet dokumentimi i të gjithë informacionit të rëndësishëm rreth incidentit, përfshirë kohën e ndodhjes, natyrën e incidentit, sistemet, shërbimet, të dhënat, ose proceset që janë të prekura dhe veprimet e ndërmarra deri në atë pikë.
3. Regjistrimi i dokumentacionit të incidentit nga operatorët mbahet sipas formatit të regjistrit të përcaktuar në Aneksin 3 pjesë e kësaj rregulloreje.

Neni 13
Regjistri i incidenteve nga AKSK

Të dhënat mbi incidentet e raportuara do të mblidhen dhe dokumentohen në regjistrin elektronik të administruar nga Autoriteti Kombëtar për Sigurinë kibernetike, sipas Aneksit 4 të kësaj rregulloreje, 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.

ANEKSI 1

Forma e raportimit të incidentit kibernetik brenda 4 orëve nga identifikimi			
Seksioni 1: Të dhënat e organizatës			
Emri i Organizatës:		Sektori:	
Lloji i infrastrukturës së informacionit:	☐ Kritike ☐ E rëndësishme		
IP publike e infrastrukturës:			
Numri i Punonjësve: ☐ 0-50 ☐ 51-100 ☐ 101-500 ☐ 500+			
A keni kontraktuar palë të treta për sigurinë e kompanisë suaj:	☐ Po ☐ Jo	Nëse po, cili është emri i kompanisë	
A aplikon organizata juaj sigurim kibernetik?	☐ Po ☐ Jo	Nëse po, cili është emri i kompanisë ku jeni të siguruar?	
Të dhënat e raportuesit			
Emër Mbiemër:		Pozicioni i punës:	
E-mail:		Cel:	
Po trajtohet incidenti nga CSIRT Sektorial	☐ Po ☐ Jo	Pika e kontaktit të CSIRT Sektorial	
Lloji i asistencës që kërkoni nga AKSK			
☐ Vetëm raportim	☐ Trajtim	☐ Rekomandime	
Seksioni 2 : Detajet e incidentit			
Data dhe ora e zbulimit të incidentit		Data dhe ora e raportimit të incidentit	
Identifikimi i incidentit			
☐ Njoftime nga pajisjet	☐ SIEM / SOC	☐ Analiza e log-eve	
☐ Njoftim nga palët e treta	☐ Njoftim nga përdoruesi	☐ Help Desk	
☐ Tjetër: _____			
Statusi aktual i incidentit			
☐ Po ndodh	☐ Po ndodh dhe është nën kontroll	☐ Ka ndodhur dhe është nën kontroll	☐ Ka ndodhur
A keni back up?	☐ Po	☐ Jo	

Kategoria e incidentit			
☐ Përmbajtje abuzive	☐ Kod keqdashës	☐ Mbledhja e informacionit	☐ Përpjekjet për ndërhyrje
☐ Ndërhyrjet	☐ Disponueshmëria	☐ Siguria e Përmbajtjes së Informacionit	
☐ Mashtrimi	☐ Vulnerabiliteti	☐ Cryptomining	
☐ Eksfiltrimi	☐ Incident në ambjent testimi		
Nënkategoria e incidentit			
Përshkrim i incidentit			
Sistemet ose asetet e prekura			
Ju lutem përfshini 5-10 rreshta të "time-stamped logs" në plain ASCII			

ANEKSI 2

Forma e raportimit të incidentit kibernetik brenda 72 orëve nga identifikimi			
Seksioni 1: Impakti i incidentit			
Numri i përdoruesve të prekur:	☐ 0-50 ☐ 51-100 ☐ 101-500 ☐ 500+		
Kohëzgjatja e incidentit:			
Shtrirja gjeografike në lidhje me zonën e prekur nga incidenti:			
Shkalla e ndërprerjes së funksionimit të shërbimit:			
Ndikim në aktivitetet ekonomike dhe shoqërore:	☐ Po ☐ Jo		
Varësia e sektorëve të tjerë nga shërbimet e ofruara të operatorit të infrastrukturës së informacionit:	☐ Po ☐ Jo		
Është ruajtur nivel i mjaftueshëm të shërbimit:	☐ Po ☐ Jo		
Impakti financiar i incidentit:			
Impakti ligjor:			
Impakti në reputacion:	☐ I ulët ☐ I mesëm ☐ I lartë ☐ Kritik		
Seksioni 2: Klasifikimi i incidentit			
Cila ishte pika hyrëse e sulmit (Initial Access Vector)?			
Keni evidenca për *priviledge escalation* apo *lateral movement* ?			
Seksioni 3: Informacione mbi aktorin e sulmit			
E njihni grupin / aktorin e sulmit?	☐ Po ☐ Jo	Nëse po, cili është emri	
Keni komunikuar me grupin e sulmit?	☐ Po ☐ Jo		
Detaje teknike			
Varianti i malware		IoC	
CVE e shfrytëzuara		Metoda e enkriptimit (në rastin e ransomware):	
Të dhëna të eksfiltruara	☐ Po ☐ Jo	Website ku janë eksfiltruar të dhënat	
Përgjigja dhe rimëkëmbja			

Është përdorur backup	☐ Po ☐ Pjesërisht ☐ Jo
Është mbyllur Initial Access vector?	☐ Po ☐ Jo
Përshkruani hapat e ndërmarrë për përgjigje ndaj incidentit	

ANEKSI 3

Regjistri i incidenteve që administrohet nga operatori		
Nr	Elementet e formatit	Shpjegim
Deri në minutën e 30 të detektimit të incidentit		
1	ID e Incidentit	Identifikuesi unik për gjurmimin e incidentit
2	Data dhe Koha e Zbulimit	Data dhe koha kur incidenti u identifikua ose u zbulua për herë të parë.
3	Metoda e Zbulimit	Si u zbulua incidenti (p.sh., sistemi i detektimit të ndërhyrjes, raportimi nga punonjësi, alarm automatik).
4	Raportuar Nga	Emri dhe informacioni i kontaktit të personit ose sistemit që raportoi incidentin.
Pas minutës së 30 të detektimit të incidentit		
5	Kategoria e Incidentit	Kategoria e incidentit kibernetik.
6	Nënkategoria e Incidentit	Nënkategoria e incidentit kibernetik.
7	Përshkrimi i Incidentit	Përshkrim i detajuar i incidentit, duke përfshirë çfarë ndodhi dhe cilat sisteme, shërbime, të dhëna, ose procese janë të prekura.
8	Asetet e Prekura	Lista e aseteve të prekura nga incidenti (p.sh., sistemet, rrjetet, pajisjet, të dhënat).
9	Niveli i Ashpërsisë	Ashpërsia e incidentit bazuar në kritere të paracaktuara (p.sh., i Ulët, Mesatar, i Lartë, Kritik).
10	Koordinatori i Incidentit	Emri dhe roli i individit përgjegjës për mbikëqyrjen e procesit të përgjigjes ndaj incidentit.
11	Ekipi i Përgjigjes së Incidentit Kibernetik	Anëtarët e ekipit të përgjigjes ndaj incidentit dhe rolet e tyre.
12	Reagimi fillestar	Veprimet e menjëhershme të ndërmarra si përgjigje ndaj incidentit (p.sh., izolimi i sistemeve të prekura, revokimi i të drejtave të aksesit etj.).

13	Komunikimi	Regjistrimi i komunikimeve gjatë incidentit, duke përfshirë njoftimet e brendshme dhe komunikimet e jashtme me palët e interesuara, klientët ose autoritetet.
14	Analiza Teknike	Analiza e detajuar e incidentit, duke përfshirë vektorët e sulmit të përdorur, dobësitë e shfrytëzuara dhe të dhënat e kompromentuara.
15	Izolimi, Fshirja dhe Rikthimi	Hapat specifikë të ndërmarrë për të izoluar incidentin, eleminuar kërcënimet dhe rikthyer sistemet e prekura në operim normal.
16	Zgjidhja dhe Mbyllja	Detajet mbi zgjidhjen e incidentit, duke përfshirë kur dhe si u rikthye operimi normal.
17	Raporti i incidentit	Raporti i incidentit dokumenton incidentin, analizon shkaqet dhe pasojat e tij, si dhe për identifikon mësime të rëndësishme që mund të ndihmojnë në parandalimin e incidenteve të ardhshme, në format të linkuar.
18	Aktiviteti Pas Incidentit	Veprimet e ndjekura si analiza pas ngjarjes, mësimet e nxjerra dhe masat për të parandaluar përsëritjen.
19	Rishikimi dhe Përditësimi	Data kur incidenti dhe procesi i përgjigjes do të rishikohen për të përditësuar politikat, procedurat dhe kontrollat bazuar në mësimet e nxjerra.

ANEKS 4

Regjistri i incidenteve që administrohet nga AKSK		
Nr	Elementet e formatit	Shpjegim
Deri në minutën e 30 të detektimit të incidentit		
1	ID e Incidentit	Identifikuesi unik për gjurmimin e incidentit
2	Infrastruktura	Infrastruktura ku ka ndodhur incidenti
3	Data dhe Koha e Zbulimit	Data dhe koha kur incidenti u identifikua ose u zbulua për herë të parë.
4	Metoda e Zbulimit	Si u zbulua incidenti (p.sh., sistemi i detektimit të ndërhyrjes, raportimi nga punonjësi, alarm automatik).
5	Raportuar Nga	Emri dhe informacioni i kontaktit të personit ose sistemit që raportoi incidentin.
Pas minutës së 30 të detektimit të incidentit		
6	Kategoria e Incidentit	Kategoria e incidentit kibernetik.
7	Nënkategoria e Incidentit	Nënkategoria e incidentit kibernetik.
8	Përshkrimi i Incidentit	Përshkrim i detajuar i incidentit, duke përfshirë çfarë ndodhi dhe cilat sisteme, shërbime, të dhëna, ose procese janë të prekura.
9	Asetet e Prekura	Lista e aseteve të prekura nga incidenti (p.sh., sistemet, rrjetet, pajisjet, të dhënat).
10	Niveli i Ashpërsisë	Ashpërsia e incidentit bazuar në kritere të paracaktuara (p.sh., i Ulët, Mesatar, i Lartë, Kritik).

11	Koordinatori i Incidentit	Emri dhe roli i individit përgjegjës për mbikëqyrjen e procesit të përgjigjes ndaj incidentit.
12	Ekipi i Përgjigjes së Incidentit Kibernetik	Anëtarët e ekipit të përgjigjes ndaj incidentit dhe rolet e tyre.
13	Reagimi fillestar	Veprimet e menjëhershme të ndërmarra si përgjigje ndaj incidentit (p.sh., izolimi i sistemeve të prekura, revokimi i të drejtave të aksesit etj.).
14	Komunikimi	Regjistrimi i komunikimeve gjatë incidentit, duke përfshirë njoftimet e brendshme dhe komunikimet e jashtme me palët e interesuara, klientët ose autoritetet.
15	Analiza Teknike	Analiza e detajuar e incidentit, duke përfshirë vektorët e sulmit të përdorur, dobësitë e shfrytëzuara dhe të dhënat e kompromentuara.
16	Izolimi, Fshirja dhe Rikthimi	Hapat specifikë të ndërmarrë për të izoluar incidentin, eleminuar kërcënimet dhe rikthyer sistemet e prekura në operim normal.
17	Zgjidhja dhe Mbyllja	Detajet mbi zgjidhjen e incidentit, duke përfshirë kur dhe si u rikthye operimi normal.
18	Raporti i incidentit	Raporti i incidentit dokumenton incidentin, analizon shkaqet dhe pasojat e tij, si dhe për identifikon mësime të rëndësishme që mund të ndihmojnë në parandalimin e incidenteve të ardhshme, në format të linkuar.
19	Aktiviteti Pas Incidentit	Veprimet e ndjekura si analiza pas ngjarjes, mësimet e nxjerra dhe masat për të parandaluar përsëritjen.
20	Rishikimi dhe Përditësimi	Data kur incidenti dhe procesi i përgjigjes do të rishikohen për të përditësuar politikat, procedurat dhe kontrollat bazuar në mësimet e nxjerra.