REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr.2007 Prot

Tiranë më 11.06.2025

UDHËZIM

Nr. 1, datë 11.06.2025

PËR

MIRATIMIN E METODOLOGJISË SË VLERËSIMIT TË RISKUT TË INFRASTRUKTURËS PAS NDODHJES SË NJË INCIDENTI KIBERNETIK

Bazuar në shkronjën "gj" të nenit 13 të ligjit nr. 25/2024 "Për sigurinë kibernetike",

UDHËZOJ:

1. Miratimin e metodologjisë së vlerësimit të riskut të infrastrukturës pas ndodhjes së një incidenti kibernetik, sipas tekstit që i bashkëlidhet këtij udhëzimi.

2. Ngarkohet Autoriteti Kombëtar për Sigurinë Kibernetike dhe operatorët e infrastrukturave të informacionit për zbatimin e këtij udhëzimi.

Ky udhëzim hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI TAFA

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

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

METODOLOGJIA PËR VLERËSIMIN E RISKUT TË INFRASTRUKTURËS PAS NDODHJES SË NJË INCIDENTI KIBERNETIK

I. DISPOZITA TË PËRGJITHSHME

1. Objekti i kësaj metodologjie është përcaktimi i rregullave nëpërmjet të cilave kryhet vlerësimi i riskut të infrastrukturës së informacionit pas ndodhjes së një incidenti të sigurisë kibernetike kur shërbimi i ofruar nga infrastruktura ka ndaluar së funksionari për më shumë se 4 orë.
2. Qëllimi i kësaj metodologjie është vlerësimi i ndikimit, vulnerabiliteteve dhe i probabilitetit që incidenti i sigurisë kibernetike të përsëritet, si dhe kryerja e veprimeve reaktive nga CSIRT-i kombëtar dhe operatorët e infrastrukturave të informacionit për reduktimin e rrezikut dhe përmirësimin e përgjigjes ndaj incidenteve kibernetike të ardhshme.
3. Kjo metodologji është nxjerrë në zbatim të shkronjës "gj" të nenit 13 të ligjit nr. 25/2024 "Për sigurinë kibernetike".
4. Kjo metodologji zbatohet nga Autoriteti Kombëtar i Sigurisë Kibernetike dhe operatorët e infrastrukturave të informacionit.
5. Termat e përdorur në këtë metodologji kanë të njëjtin kuptim me termat e përcaktuar në ligjin nr. 25/2024 "Për sigurinë kibernetike".

II. FAZAT PËR VLERËSIMIN E RISKUT TË INFRASTRUKTURËS SË INFORMACIONIT PAS NDODHJES SË INCIDENTIT KIBERNETIK

1. Metodologjia për vlerësimin e riskut të infrastrukturës së informacionit pas ndodhjes së incidentit kibernetik përfshin fazat si vijon:

1.1. Identifikimi dhe dokumentimi i incidentit kibernetik

Kjo fazë përfshin procesin e identifikimit dhe dokumentimit të incidentit të sigurisë kibernetike me qëllim vlerësimin e natyrës dhe shkallës së incidentit kibernetik, nëpërmjet hapave si vijon:

- Përshkrimi i incidentit kibernetik duke përfshirë datën dhe orën kur ka ndodhur incidenti kibernetik.
- Identifikimi i llojit të incidentit kibernetik (p.sh. ransomware, shkelje e të dhënave, sulm DDoS).
- Identifikimi i sistemeve, aseteve të prekura dhe shërbimeve që janë ndërprerë.

- Dokumentimi i mënyrës së zbulimit të incidenti kibernetik (monitorimi i sigurisë, raportimi i përdoruesve, etj.).

1.2. Vlerësimi i vulnerabiliteteve

Kjo fazë përfshin vlerësimin e vulnerabiliteteve me qëllim identifikimin e sulmit kibernetik të ndodhur si dhe dobësitë që janë shfrytëzuar, nëpërmjet hapave si vijon:

- Analizimi i pikave të hyrjes që janë përdorur nga sulmuesit.
- Përcaktimi nëse sistemi ka pasur dobësi teknike, të tilla si:
  - Sisteme të papërditësuara, mungesë autentifikimi me shumë faktor ose software me dobësi të njohura.
  - Politika të dobëta të sigurisë për menaxhimin e fjalëkalimeve ose aksesit të privilegjuar.
  - Trajnim i pamjaftueshëm i stafit për të dalluar sulmet *phishing* apo *social engineering.*

1.3. Vlerësimi i ndikimit të incidentit kibernetik

1.3.1 Kjo fazë përfshin vlerësimin e ndikimit të incidentit kibernetik me qëllim përcaktimin e efekteve të incidentit kibernetik mbi operacionet dhe asetet kritike të infrastrukturës së informacionit. Ky vlerësim përfshin hapat si vijon:

- Ndikimi mbi operacionet: Vlerësimi nëse incidenti kibernetik ka shkaktuar ndërprerje në ofrimin e shërbimeve kritike.
- Humbja e të dhënave: Identifikimi nëse të dhënat janë vjedhur, ndryshuar, ose humbur përgjithmonë. Klasifikimi i të dhënave të prekura (personale, financiare, tregtare).
- Ndikimi financiar: Llogaritja e humbjeve financiare që kanë ardhur si rezultat i ndërprerjes së shërbimeve, dëmtimit të reputacionit, masat administrative, ose kostoja e riparimeve.
- Ndikimi reputacional: Vlerësimi i ndikimit që incidenti kibernetik ka pasur mbi besimin e klientëve dhe bashkëpunëtorët.

1.3.2 Përcaktimi i vlerësimit të ndikimit të incidentit të sigurisë kibernetike do të bëhet bazuar në tabelën si më poshtë vijon:

Kategorizimet (Llojet) e incidenteve	Përshkrim (Ndikimi)
INCIDENTET KIBERNETIKE ME NDIKIM TË ULËT	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.

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 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.

- **I ulët:** Ndikim minimal mbi operacionet ose të dhënat e infrastrukturës së informacionit.
- **Mesatar:** Ndikim i rëndësishëm, por i përmbajtur në disa shërbime të infrastrukturës së informacionit.
- **I lartë:** Ndikim madhor mbi operacionet kritike ose rrjedhje të dhënash sensitive me pasoja të rënda.

1.4. Vlerësimi i probabilitetit të përsëritjes së incidentit kibernetik

1.4.1 Kjo fazë përfshin vlerësimin e probabilitetit të përsëritjes së incidentit kibernetik me qëllim parandalimin e ndodhjes së tij në të ardhmen. Ky vlerësim përfshin hapat si vijon:

- Historiku i incidentit kibernetik: A është ky një incident i izoluar apo ka një model të përsëritur?
- Masat mbrojtëse aktuale: A janë masat e sigurisë të mjaftueshme për të parandaluar një incident të ngjashëm në të ardhmen?
- Përmirësimet e mundshme: A janë identifikuar dhe zbatuar përmirësime të sigurisë pas incidentit kibernetik?

1.4.2 Përcaktimi i mundësisë (probabilitetit) të përsëritjes së incidentit kibernetik do të kryhet sipas indikatorëve si më poshtë:

Mundësia (Probabiliteti)	Përshkrimi
I Ulët	Ekziston mundësi e ulët që të ndodhë
Mesatar	Ka një mundësi të mirë që të ndodhë
I Lartë	Pothuajse i sigurt që mund të ndodhë

1.5. Analiza e riskut kibernetik

15.1 Kjo fazë përfshin analizën e riskut kibernetik me qëllim përcaktimin e riskut të përgjithshëm që infrastruktura e informacionit përballet pas ndodhjes së incidentit kibernetik.

1.5.2 Për të përcaktuar nivelin e përgjithshëm të riskut të infrastrukturës së informacionit do të vlerësohet nëpërmjet kombininimit të ndikimin dhe probabilitetit të përsëritjes së incidentit kibernetik.

$$\text{Risku} = \text{Ndikimi} \times \text{Probabiliteti}$$

Matrica e rrezikut:

Risku = Mundësia e Ndodhjes * Ndikimi

NDIKIMI	**MUNDËSIA**			
		I Ulët (1)	**Mesatar (2)**	**Lartë (3)**
	I Ulët (1)	**I Ulët (1)**	**I Ulët (2)**	**Mesatar (3)**
	Mesatar (2)	**I Ulët (2)**	**Mesatar (4)**	**Lartë (6)**
	Lartë (3)	**Mesatar (3)**	**Lartë (6)**	**Lartë (9)**

Vlera dhe niveli i riskut:

Vlera e Riskut	Niveli i Riskut
[1-2]	I Ulët
[3-4]	Mesatar
[6-9]	Lartë

1.6. Kategorizimi i incidenteve dhe niveli i riskut

Duke analizuar llojin e incidentit si dhe infrastrukturën e prekur, përcaktohet dhe niveli i riskut të tij sipas tabelës së mëposhtme:

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		Shtrembërim 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 passëords, 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 aplikacioni (shërbimi). Ky incident mund të shkaktohet nga nga një vulnerabilitet i njohur ose i ri, por edhe nga aksesi lokal i paautorizuar.
5	**Ndërhyrjet**	Kompromentim i llogarive të paprivilegjuara		Kompromentim aplikacioni (shërbimi). Ky incident mund të shkaktohet nga nga një vulnerabilitet i njohur ose i ri, por edhe nga aksesi lokal i paautorizuar.
		Kompromentim i një aplikacioni që ofron shërbim kritik	Kompromentim i një aplikacioni që ofron shërbime të tjera	Psh ekzekutimi i teknikave injection si: SQL Injection, Command Injection, File Injection, XSS, CSRF, RCE, API attack etj.
6	**Disponueshmëria**	DoS/DDoS që ka ndërprerë sherbime kritike		

				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.
		DoS/DDoS që ka ndikuar ndjeshëm shërbimet kritike dhe/ose ka ndërprerë shërbimet e tjera		
		DoS/DDoS që nuk ka ndikim në shërbime kritike, por ka ndikuar ndjeshëm tek shërbimet e tjera.		
		Sabotimi që ka prekur sistemin kritik	Sabotimi që ka prekur sisteme të tjera.	
		Ndërprerje e shërbimeve si pasojë e një incidenti gjatë procesit të mirëmbajtjes ose/edhe teknike si: Energjia/Zjarri/Përmbytje që ka prekur infrastrukturën kritike	Ndërprerje e shërbimeve si pasojë e procesit të mirëmbajtjes ose/edhe teknike si: Energjia/Zjarri/ Përmbytje që ka prekur shërbime të tjera	
		Ndërprerje për shkak të katastrofave natyrore që ka prekur infrastrukturën kritike	Ndërprerje për shkak të katastrofave natyrore për shërbime të tjera	

7	**Siguria e Përmbajtjes së Informacionit**	Akses i paautorizuar në shërbime kritike	Akses i paautorizuar në shërbime të tjera	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 (ëiretapping, spoofing or hijacking). Këto sulme mund të shkaktohen nga gabimet njerëzore, të konfigurimit, ose erore të softuerit.
		Modifikimi i paautorizuar në shërbime kritike	Modifikimi i paautorizuar në shërbime të tjera	
8	**Mashtrimi**	Përdorimi i paautorizuar i burimeve		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.
		E drejta e autorit		Ofrimi ose instalimi i kopjeve të softuerit komercial të paliçensuar ose materialeve të tjera të mbrojtura nga e drejta e autorit.
		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/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 ambient testimi**	Incident i ndodhur në ambient 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 à Marrjen leje të dhënave, dhe në fund shkatërrimin e tyre në mënyrë të përhershme.

1.7. Përcaktimi i masave korrigjuese dhe parandaluese

Kjo fazë përfshin përcaktimin e masave korrigjuese dhe parandaluese me qëllim përmirësimin e sigurisë në infrastrukturën e informacionit si dhe parandalimin e përsëritjes së incidentit kibernetik në të ardhmen. Kjo fazë përfshin:

- Përmirësimet teknike: Zbatimi i masave mbrojtëse të tilla, si firewall më të fuqishëm, IDS/IPS, rritja e nivelit të enkriptimit dhe përmirësimi i politikave të fjalëkalimeve.
- Politikat dhe procedurat: Rishikimi dhe përmirësimi i politikave të sigurisë për menaxhimin e të dhënave dhe aksesit.
- Trajnimi i stafit: Rritja e ndërgjegjësimit të stafit nëpërmjet trajnimeve të vazhdueshme dhe periodike të cilat përfshijnë simulime të rregullta të sulmeve phishing, workshope për menaxhimin e fjalëkalimeve të sigurta, programe të ndërgjegjësimit për kërcënimet e reja si sulmet me AI etj.
- Monitorimi i përhershëm: Monitorim i vazhdueshëm për zbulimin e anomalive dhe shenjave të sulmeve të mundshme të ardhshme.

1.8. Rekomandime, plani i rimëkëmbjes dhe raportimi

Kjo fazë përfshin dhënien e rekomandimeve, masat që duhet të ndërmerren për rimëkëmbjen nga incidenti i sigurisë kibernetike si dhe raportimi me qëllim vlerësimin dhe dokumentimin e rezultateve dhe veprimeve. Kjo fazë përfshin:

- Raportin përfundimtar: Përgatitja e një raporti përfundimtar që përfshin përshkrimin e incidentit kibernetik, ndikimin, riskun, dhe masat e ndërmarra, rekomandimet për vazhdimesinë.
- Ndjekja e masave të zbatuara: Masat korrigjuese dhe parandaluese janë zbatuar dhe janë efektive.
- Raportimi te palët e interesuara: Informimi i palëve të interesuara për incidentin kibernetik dhe masat e marra.
- Plan i rimëkëmbjes: Hartimi i një plani për rimëkëmbjen e shpejtë të shërbimeve dhe rikthimin e besimit të përdoruesve.