VENDIM
Nr. 814, datë 30.12.2025

PËR MIRATIMIN E PROCEDURAVE TË IDENTIFIKIMIT, KLASIFIKIMIT, PËRSHKALLËZIMIT DHE MENAXHIMIT TË KRIZËS KIBERNETIKE

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 9, të nenit 28, të ligjit nr. 25/2024, "Për sigurinë kibernetike", me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e procedurave të identifikimit, klasifikimit, përshkallëzimit dhe menaxhimit të krizës kibernetike, sipas tekstit që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.
2. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, CSIRT-et sektoriale, CSIRT-et pranë operatorëve të infrastrukturave të informacionit dhe të gjitha strukturat e institucionet përgjegjëse, që kanë role dhe përgjegjësi specifike të përcaktuara në procedurën e identifikimit, klasifikimit, përshkallëzimit dhe menaxhimit të krizës kibernetike, për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

PROCEDURAT PËR IDENTIFIKIMIN, KLASIFIKIMIN, PËRSHKALLËZIMIN Dhe MENAXHIMIN E KRIZËS KIBERNETIKE

1. HYRJE

Rritja e përdorimit të teknologjive digjitale të informacionit e të komunikimit, si dhe e shërbimeve digjitale ka bërë që edhe kërcënimet ndaj sigurisë kibernetike të jenë gjithnjë e më të pranishme e të sofistikuara. Ky fenomen, tashmë global, nuk njeh kufij, duke e bërë menaxhimin e incidenteve dhe krizave kibernetike një sfidë të rëndësishme për të gjitha shtetet. Incidentet e sigurisë kibernetike mund të përfshijnë, që nga sulmet e thjeshta deri tek sulmet më të sofistikuara, me pasojë ndërprerjen e shërbimeve kritike, vjedhjen e informacionit sensitiv apo shkatërrimin e infrastrukturave kritike dhe të rëndësishme të informacionit.

Pas një rritjeje të ndjeshme të sulmeve kibernetike, kuadri ligjor për menaxhimin dhe reagimin ndaj incidenteve kibernetike, në shkallë të gjerë me përshkallëzim në krizë kibernetike, është një instrument për të siguruar që Shqipëria të jetë e përgatitur për të përballuar çdo incident apo krizë të mundshme të sigurisë kibernetike, duke mbrojtur infrastrukturat kritike e të rëndësishme të informacionit dhe duke siguruar vazhdimësinë e shërbimeve kyçe. Për të siguruar një menaxhim të koordinuar dhe efikas të incidenteve në shkallë të gjerë dhe krizave kibernetike është e rëndësishme të përfshihen të gjithë aktorët relevantë, qeveria, institucione të pavarura, sektori privat dhe shoqëria civile. Nëpërmjet bashkëpunimit, koordinimit dhe trajnimit të vazhdueshëm në fushën e sigurisë kibernetike, do të bëhet e mundur që Shqipëria të përballet me sfidat e sigurisë kibernetike, si dhe të reagojë në mënyrë të shpejtë dhe efikase, me qëllim minimizimin e pasojave. Hartimi i kësaj procedure ka si qëllim krijimin e një kornize gjithëpërfshirëse e të strukturuar për identifikimin, klasifikimin, menaxhimin ndaj krizave të sigurisë kibernetike që mund të rrezikojnë funksionimin normal të shoqërisë dhe ekonomisë shqiptare.

Kapaciteti efektiv i menaxhimit të krizave kibernetike varet nga kapacitetet efektive në nivel strategjik politik, operacional dhe teknik, si dhe bashkëpunimit të ngushtë ndërmjet këtyre niveleve, ashtu siç theksohet në rekomandimin e Komisionit Evropian (BE) 2017/1584, datë 13 shtator 2017, mbi reagimin e koordinuar ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike.

Menaxhimi i krizës kibernetike kombëtare përfshin shumë aktorë, si: ministri, autoritete

rregullatore, institucione të pavarura, institucione ligjzbatuese etj., pasi ato udhëheqin përpjekjet mbrojtëse të shtetit për të përballuar sulmet dhe pasojat e tyre. Qëndrueshmëria kibernetike është aftësia për të ruajtur vazhdimësinë e shërbimeve kritike e të rëndësishme për vendin, pavarësisht ashpërsisë së goditjeve kibernetike drejt infrastrukturave të tyre të informacionit.

Në këtë kuadër, ky dokument synon:

- të përcaktojë proceduarat për identifikimin, klasifikimin, përshkallëzimin dhe menaxhimin e krizës kibernetike;
- të sigurojë koordinimin dhe bashkëpunimin ndërmjet institucioneve shtetërore, sektorit privat dhe organizatave ndërkombëtare për të krijuar një rrjet të sigurt dhe të besueshëm për përgjigjen dhe menaxhimin e krizave kibernetike, për të ndihmuar në minimizimin e pasojave, si dhe për të siguruar shkëmbimin e shpejtë dhe efikas të informacionit dhe të masave mbrojtëse midis aktorëve të përfshirë në fushën e sigurisë kibernetike, institucioneve dhe shteteve;
- të përgatitë institucionet dhe infrastrukturat kritike e të rëndësishme të informacionit për të reaguar ndaj krizave të sigurisë kibernetike, përfshirë masat për parandalimin e përshkallëzimit të incidenteve kibernetike në shkallë të gjerë dhe mësimet e nxjerra nga situatat e mëparshme;
- të rritë kapacitetet e reagimit e të ndërhyrjes për të menaxhuar me sukses situata të krizës së sigurisë kibernetike dhe për të garantuar vazhdimësinë e funksioneve dhe të shërbimeve kritike e të rëndësishme të infrastrukturave të informacionit.

2. PROCEDURAT PËR IDENTIFIKIMIN, KLASIFIKIMIN, PËRSHKALLËZIMIN DHE MENAXHIMIN EFEKTIV TË KRIZËS KIBERNETIKE

2.1 Kriza kibernetike

Krizë kibernetike është situata gjatë së cilës siguria e informacionit në sistemet e informacionit ose siguria e rrjeteve të komunikimeve elektronike është seriozisht e rrezikuar, duke vënë në rrezik interesin publik të Republikës së Shqipërisë.

Identifikimi, përshkallëzimi dhe menaxhimi i krizës kibernetike bazohen në dokumentin e ENISA-s "Për bashkëpunimin dhe menaxhimin e krizave kibernetike". Sipas ENISA-s, kriza kibernetike fillon kur një incident i zakonshëm kibernetik shndërrohet në një ngjarje të jashtëzakonshme, që do të thotë se ai ndryshon nga normalja dhe përfshin shqetësim serioz ose rrezik për bllokimin e funksioneve jetësore të shoqërisë.

Kriza kibernetike trajtohet duke u bazuar në këto dy elemente themelore, të vlerësuar në ndërveprim me rrethanat në hapësirën kibernetike dhe atë fizike:

1. Vlerësohet potenciali i një incidenti kibernetik për të shkaktuar dëme reale, për të ndërprerë ose për të kompromet uar vazhdimësinë funksionale të shërbimeve kritike e të rëndësishme të infrastrukturave të informacionit, si dhe për t'u përshkallëzuar në një gjendje të jashtëzakonshme kombëtare.
2. Në rastet e situatave emergjente të shkaktuara nga faktorë fizikë jokibernetikë, si konflikte të armatosura, akte terroriste apo fatkeqësi natyrore, merret në konsideratë rritja e nivelit të rrezikut për shpërthimin e një krize kibernetike dhe intensifikimi i aktivitetit keqdashës kibernetik.

2.2 Fazat e krizës kibernetike

Kriza kibernetike kalon në disa faza:

- Faza e alarmit në një krizë kibernetike;
- Faza e vlerësimit të situatës dhe identifikimit të krizës kibernetike;
- Faza e përgjigjes dhe menaxhimit të krizës kibernetike;
- Faza e rimëkëmbjes pas krizës kibernetike.

2.2.1 Faza e alarmit në një krizë kibernetike

Faza e alarmit në një krizë kibernetike është momenti kur incidenti kibernetik i identifikuar vlerësohet si kërcënim serioz, që mund të ndikojë në funksionimin normal të sistemit ose të infrastrukturës së informacionit, duke kërkuar aktivizimin e menjëhershëm të strukturave të reagimit. Në këtë fazë, konfirmohet karakteri kritik i ngjarjes, përcaktohet niveli i alarmit,

sipas protokolleve të brendshme, dhe njoftohen aktorët kyç operativë dhe vendimmarrës, përfshirë ekipet teknike, menaxhimin e lartë, si dhe autoritetet kombëtare kompetente, me qëllim koordinimin e shpejtë e të strukturuar, që të parandalohet përhapja e dëmeve dhe të fillojë menaxhimi aktiv i situatës në kohë reale.

Gjendjet e alarmit kibernetik përcaktohen dhe përdoren si mekanizëm formal për vlerësimin e nivelit të vigjilencës e të gatishmërisë institucionale për përballimin e rreziqeve në hapësirën kibernetike e fizike. Autoriteti, në koordinim me infrastrukturën e informacionit të prekur, përcakton gjendjen e alarmit kibernetik mbi bazën e vlerësimit të situatës, i cili mbështetet në informacione të verifikuara, fakte e analiza të përbashkëta teknike dhe operacionale. Në përputhje me nivelin e incidentit kibernetik të konstatuar, autoriteti ngre gjendjen përkatëse të alarmit kibernetik dhe aktivizon procedurat përkatëse të reagimit, duke siguruar funksionimin e mekanizmave të koordinimit e të ndërhyrjes. Me shpalljen e gjendjes së alarmit kibernetik, subjektet përgjegjëse zbatojnë menjëherë masat dhe veprimet e përcaktuara për nivelin përkatës të alarmit, me qëllim kufizimin e ndikimit të incidentit dhe reduktimin e rrezikut të dëmtimit të infrastrukturës së informacionit.

Shpallja në kohë e gjendjes së alarmit kibernetik është e detyrueshme dhe synon parandalimin e përshkallëzimit të incidenteve kibernetike në krizë kibernetike, si dhe kufizimin e dëmeve, në rastet kur kriza kibernetike është identifikuar.

Mosshpallja ose vonesa në shpalljen e gjendjes së alarmit kibernetik rrit rrezikun e shkaktimit të dëmeve në shkallë të gjerë ndaj infrastrukturave të informacionit dhe të vazhdimësisë së shërbimeve kritike.

2.2.1.1 Skema e përshkallëzimit të gjendjes së alarmit kibernetik

Skema e përshkallëzimit të gjendjes së alarmit kibernetik përcaktohet sipas tabelës 1, të kësaj procedure, dhe zbatohet nga Autoriteti dhe nga subjektet përgjegjëse, në përputhje me nivelin e rrezikut dhe ndikimit të incidentit kibernetik.

Situatë e mbrojtjes rutinë – Në mungesë të shpalljes së një gjendjeje alarmi kibernetik, infrastruktura kritike e informacionit konsiderohet në gjendje të mbrojtjes rutinë dhe është e detyruar të zbatojë masat standarde të sigurisë kibernetike, të kryejë operacione rutinë dhe të përditësojë planet e mbrojtjes kibernetike, pa konstatuar ndërprerje të funksionimit normal të infrastrukturës së informacionit.

Situatë e përshkallëzimit të nivelit fillestar – Aktivizohet kur konstatohet një kërcënim i rëndësishëm ndaj një shërbimi kritik ose rrezik për ndërprerjen e funksionimit normal të infrastrukturës së informacionit, edhe nëse origjina kibernetike e kërcënimit nuk është ende e konfirmuar.

Situatë e përshkallëzimit të nivelit mesatar – Aktivizohet kur konstatohet dëmtim i infrastrukturave kritike të informacionit, që cenon në mënyrë të konsiderueshme vazhdimësinë e proceseve kryesore.

Situatë e përshkallëzimit të nivelit të lartë – Aktivizohet kur ndodh një dëmtim i zgjatur në kohë dhe në shkallë të gjerë ndaj infrastrukturave kritike të informacionit, duke shkaktuar dëme të mëdha në proceset bazë dhe në vazhdimësinë e funksionimit të shërbimeve të infrastrukturës së informacionit të prekur.

Faza	Përshkrimi
Mbrojtja rutinë	Niveli i mbrojtjes rutinë: nuk ka tregues të ndërprerjes së vazhdimësisë funksionale të shërbimeve kritike të infrastrukturës së informacionit.
Përshkallëzimi	Niveli fillestar: kërcënim thelbësor për një shërbim kritik të infrastrukturës së informacionit. Vazhdimësia funksionale e një shërbimi kritik të infrastrukturës së informacionit mund të rrezikohet.
	Niveli mesatar: dëmtimi i shërbimeve kritike të infrastrukturës së informacionit mund të shkaktojë mosfunksionim të konsiderueshëm në vazhdimësinë e proceseve kryesore.
	Niveli i lartë: dëmtimi i zgjatur në kohë dhe në shkallë të gjerë ndaj shërbimeve kritike të infrastrukturës së informacionit shkakton dëme të konsiderueshme në proceset kritike dhe në vazhdimësinë e funksionimit të shërbimeve.

Tabela 1: Skema e përshkallëzimit të alarmit kibernetik.

2.2.1.2 Treguesit për përcaktimin e gjendjes së alarmit kibernetik në hapësirë kibernetike dhe fizike

Gjendja e alarmit kibernetik përcaktohet mbi bazën e vlerësimit të rrezikut nëpërmjet treguesve të ashpërsisë së kërcënimit dhe mundësive të materializimit të tyre, duke analizuar veprimet që duhet të ndërmerren, si dhe burimet e mjetet që duhet të përdoren. Emergjencat e shkaktuara nga një faktor jokibernetik (si: lufta, fenomeni natyror, aktivitetet terroriste, keqfunksionimi, etj.) shpesh shërbejnë si mundësi për sulmuesit kibernetikë për të rritur përpjekjet e tyre, pikërisht, kur funksionimi normal i shërbimeve kritike të infrastrukturës së informacionit bëhet edhe më thelbësor, gjendja e alarmit kibernetik do të përcaktohet jo vetëm nga rrethanat në hapësirën kibernetike, por edhe nga rrethanat në hapësirën fizike.

Në lidhje me korrelacionin midis treguesve dhe gjendjeve të alarmit kibernetik, veprimet dhe vlerësimet kryhen sipas këtyre parimeve:

1. Përdorimi i treguesve: Një tregues i caktuar nuk përcakton automatikisht një nivel specifik të alarmit kibernetik. Treguesit shërbejnë si mjete për vlerësimin e situatës për të ndihmuar në përcaktimin e nivelit të alarmit.

2. Shpallja e alarmit para incidentit: Një alarm kibernetik mund të aktivizohet edhe pa konstatimin e një dëmtimi konkret të shërbimeve kritike. Aktivizimi mund të bazohet në sinjalizime të shërbimeve të inteligjencës mbi rreziqe të mundshme ose në rrethanat që rrisin rëndësinë e funksionimit normal të infrastrukturës së informacionit. Në këtë mënyrë, mund të përcaktohet një nivel alarmi (p.sh., A ose B), si rezultat i një incidenti me ndikim të ulët ose të konsiderueshëm, veçanërisht gjatë emergjencave të shkaktuara nga faktorë jokibernetikë, duke ruajtur në të njëjtën kohë masat e mbrojtjes rutinë.

2.2.1.3 Gjendjet e alarmit kibernetik dhe treguesit për përcaktimin e secilit nivel

Mbrojtja rutinë: Përfaqëson situatën e paracaktuar, kur rrethanat në hapësirën kibernetike dhe në hapësirën fizike nuk shfaqin tregues për një ndërprerje të funksionimit normal të infrastrukturës së informacionit ose ndonjë nevojë për të rritur nivelin e mbrojtjes. Në këto rrethana, nuk ka tregues për nivele të larta alarmi.

Treguesit në hapësirën kibernetike përcaktojnë nëse kanë ndodhur incidente të dukshme kibernetike, por pa ndërprerë funksionimin e infrastrukturës së informacionit ose nuk kanë ndodhur incidente të dukshme kibernetike.

Treguesit në hapësirën fizike përcaktojnë alarme të përgjithshme për mundësinë e ndodhjes së incidenteve kibernetike.

Niveli A i alarmit kibernetik: Niveli A i alarmit kibernetik (incident në nivel të ulët) përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- *Treguesit në hapësirën kibernetike:*

- *Paralajmërim për një incident kibernetik:* Ka ndodhur një incident kibernetik i izoluar, i cili tregon për ndërprerje të mundshme të funksionimit normal të një shërbimi jokritik në një operator të infrastrukturës së informacionit, por nuk ka tregues që prekin të gjithë sektorin apo degë të operatorit të infrastrukturës së informacionit;

- *Marrja e një alarmi informativ:* Informacion lidhur me një kërcënim, dobësi në sistemet e informacionit, të cilat mund të prekin një ose disa shërbime jokritike të operatorit të infrastrukturës së informacionit;

- *Ngjarje botërore që prekin direkt ose indirekt Republikën e Shqipërisë:* Sulme kibernetike që ndodhin jashtë territorit të Republikës së Shqipërisë, por që prekin direkt apo indirekt shtetin tonë, p.sh. sulme kibernetike ndaj kompanive që kanë filiale në vendin tonë ose sulme ndaj vendeve aleate.

- *Treguesit në hapësirën fizike:*

- *Problem operacional ose teknik:* Një mosfunksionim operacional ose teknik në një shërbim jokritik dhe/ose në vendin ku infrastruktura përkatëse e informacionit ndodhet;

-*Ngjarje botërore që prekin indirekt Shqipërinë:* Paralajmërimi i një ngjarjeje jonormale sigurie (si p.sh. një përshkallëzim i lëshimit të raketave drejt vendeve aleate).

Niveli B i alarmit kibernetik: Niveli B i alarmit kibernetik përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- *Treguesit në hapësirën kibernetike:*

- *Paralajmërim për një sulm kibernetik:* CSIRT-i kombëtar informohet nga shërbimet e inteligjencës, CSIRT-et e shteteve aleate ose organizata ndërkombëtare për sulme të mundshme kibernetike drejt një shërbimi të një sektori kritik;

- *Dëmtimi i shërbimeve kritike si pasojë e sulmit kibernetik*: Rezultati konsiston në ndërprerjen e mundshme të vazhdimësisë së një shërbimi kritik të infrastrukturës së informacionit, por nuk ka të dhëna për përhapje në të gjithë sektorin.

- *Treguesit në hapësirën fizike:*

- *Dëmtime fizike:* Dëmtime fizike të shërbimeve që janë kritike (si: ndërprerja e energjisë elektrike, ndërprerja e shërbimeve shëndetësore), por që janë të lokalizuara vetëm në një operator të infrastrukturës së informacionit;

- *Ngjarje botërore që prekin drejtpërdrejt Shqipërinë:* Një sulm i ndodhur diku në një vend tjetër, por që i atribuohet Shqipërisë.

Niveli C i alarmit kibernetik: Niveli C i alarmit kibernetik është niveli i lartë i alarmit kibernetik, ku rrethanat që nxitën shpalljen e kësaj gjendjeje mund të përshkallëzohen deri në një gjendje emergjence kombëtare. Niveli C i alarmit kibernetik përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- *Treguesit në hapësirën kibernetike*:

- *Dëmtime të disa shërbimeve kritike, si pasojë e sulmeve kibernetike*: Dëmtime ndaj disa shërbimeve kritike të operatorit të infrastrukturës së informacionit, të cilat çojnë në ndërprerje të disa proceseve bazë dhe në vazhdimësinë funksionale të ekonomisë (siç është dëmtimi ndërsektorial);

- *Treguesit në hapësirën fizike:*

- *Dëmtime fizike të vazhdueshme:* Dëmtime fizike të disa infrastrukturave, shërbimeve që janë të rëndësishme për ekonominë e vendit;

- *Përgatitje për fillimin e një lufte:* Përgatitje serioze për luftë ose një operacion ushtarak në shkallë të gjerë.

Niveli D i alarmit kibernetik: Niveli D është gjendja e emergjencës kombëtare, që është niveli më i lartë i alarmit kibernetik. Niveli D i alarmit kibernetik përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- *Treguesit në hapësirën kibernetike*:

- *Dëmtime në shkallë të gjerë të shërbimeve kritike si pasojë e sulmeve kibernetike*: Dëmtime të mëdha dhe/ose të vazhdueshme ndaj shërbimeve kritike të operatorit të infrastrukturës kritike e të rëndësishme të informacionit, të cilat çojnë në ndërprerje të shumë shërbimeve bazë jetësore, si edhe të ekonomisë (siç është dëmtimi ndërsektorial).

- *Indikatorët në hapësirën fizike:*

- *Dëmtime fizike të vazhdueshme:* Dëmtime fizike të shumta dhe/ose të vazhdueshme ndaj infrastrukturave të informacionit që mundësojnë ofrimin e shërbimeve, që janë të rëndësishme për ekonominë e vendit;

- *Situata e një lufte:* Luftë ose një operacion ushtarak në shkallë të gjerë;

- *Gjendja e jashtëzakonshme:* Shpallja e një gjendjeje të jashtëzakonshme, e kushtëzuar me qëndrimin në shtëpi "/"ngjarje emergjence civile".

Figura 1 Treguesit e përcaktimit të secilit nivel

2.2.1.4 Përcaktimi i gjendjes së alarmit kibernetik përcaktohet nga Autoriteti pas koordinimit me infrastrukturën e prekur, bazuar në një raport të vlerësimit të situatës.

2.2.1.5 Parimet për ndryshimin e gjendjes së alarmit kibernetik

Gjatë çdo gjendjeje alarmi, çdo infrastrukturë informacioni kryen një vlerësim të situatës, shqyrton treguesit në hapësirën kibernetike dhe në hapësirën fizike e më pas konstaton nëse ka nevojë për të ndryshuar gjendjen e alarmit.

Rritja e nivelit të alarmit kibernetik:

Rritja e nivelit të alarmit kibernetik ndikohet nga përshkallëzimi i situatës në rrethana të caktuara dhe kërkon ndërmarrjen e veprimeve të mëtejshme ose intensifikimin e masave tashmë të zbatuara. Qëllimi i këtyre veprimeve është të parandalohet përkeqësimi i situatës ose të minimizohen dëmtimet e mundshme.

- Rritja graduale e alarmit: Niveli i alarmit duhet të përcaktohet dhe të rritet gradualisht, bazuar në treguesit e situatës, duke analizuar çdo ndryshim në rrezikun ose ndikimin e mundshëm në shërbimet kritike.

- Përjashtimet: Në situata ekstreme, mund të shpallet menjëherë niveli i emergjencës kibernetike, pa kaluar përmes niveleve të tjera të alarmit, për të garantuar ndërhyrje të menjëhershme dhe mbrojtje të vazhdueshme të infrastrukturës kritike.

Ulja e nivelit të alarmit kibernetik:

Niveli i alarmit kibernetik ulet nëse treguesit përkatës, që çuan në përcaktimin e nivelit të alarmit, nuk janë më të pranishëm. Niveli i alarmit ulet gradualisht, nga një kategori çdo herë, derisa të rikthehet mbrojtja kibernetike rutinë.

1.2.1 Faza e vlerësimit të situatës dhe identifikimit të krizës kibernetike

Faza e vlerësimit të situatës dhe identifikimit të krizës kibernetike zhvillohet si më poshtë:

Fillimi i vlerësimit: Vlerësimi i situatës nis sapo gjendja e alarmit kibernetik arrin nivelin C. Kjo përfshin analizën e shkaqeve, shtrirjes dhe ndikimit të mundshëm të incidenteve kibernetike në shkallë të gjerë për operatorët e infrastrukturave të informacionit.

Përshkallëzimi i alarmit: Nëse nga analiza rezulton se gjendja e alarmit është rritur nga niveli C në nivelin D (emergjencë kibernetike) dhe në të njëjtën kohë shërbimet kritike të operatorit janë ndërprerë, duke cenuar rëndë sigurinë e informacionit dhe nuk mund të rikthehen brenda një afati të përcaktuar, situata konsiderohet për identifikimin e krizës kibernetike.

Identifikimi i krizës kibernetike: Kriza kibernetike përcaktohet, sipas rastit, duke marrë parasysh:

a) Shkallën e ndikimit për shërbimet kritike;

b) Kohëzgjatjen e ndërprerjes së funksionimit normal;

c) Pamundësinë për rikthim të shpejtë të sigurisë dhe funksionalitetit të infrastrukturës.

Kriza kibernetike mund të identifikohet, sipas rastit:

Në nivel kombëtar – Kriza kibernetike identifikohet pas një kërcënimi ose rrethanash që mund të përshkallëzohen deri në një gjendje emergjence kombëtare/krize kibernetike, ku janë përfshirë disa sektorë kritikë ose të gjithë sektorët kritikë të ekonomisë, me shtrirje në nivel kombëtar.

Në nivel sektorial – Kriza kibernetike identifikohet pas një kërcënimi ose rrethanash që mund të përshkallëzohen deri në një gjendje emergjence kombëtare/krize kibernetike, edhe për një nga sektorët jetikë me shtrirje dhe ndikim kombëtar (p.sh. është përfshirë sektori i energjisë, i cili ka paralizuar gjithë sektorët e tjerë). Shpallja e gjendjes së krizës kibernetike në nivel sektorial bën të detyrueshëm që të gjitha strukturat, që janë pjesë e atij sektori, të kalojnë në gjendje alarmi. Shpallja e gjendjes së alarmit kibernetik në një sektor të caktuar nuk është detyruese për sektorët e tjerë, por tregon se ekzistojnë rrethana të caktuara në hapësirën kibernetike, të cilat duhet të adresohen edhe nga sektorët e tjerë.

2.2.2.1 Hapat për shpalljen e gjendjes së krizës kibernetike

1. Kur Autoriteti merr njoftim për një incident të rëndë të sigurisë kibernetike, që ka ndikim dhe shtrirje të gjerë në operatorët e infrastrukturave kritike të informacionit, Autoriteti fillon një vlerësim paraprak mbi incidentin për të përcaktuar ndikimin politik, ekonomik dhe të sigurisë.
2. Pas vlerësimit të situatës, Autoriteti harton një raport paraprak.
3. Kur nga raporti paraprak arrihet në përfundimin se situata konsiston në një krizë të mundshme kibernetike, Autoriteti njofton menjëherë subjektet e tjera përgjegjëse të sigurisë dhe mbrojtjes, sipas shkronjës "a", të nenit 11, të ligjit nr. 25/2024, "Për sigurinë kibernetike", duke filluar një proces koordinues dhe konsultues për vlerësimin e situatës në nivel kombëtar.
4. Pas një vlerësimi të koordinuar me subjektet e tjera përgjegjëse të sigurisë dhe mbrojtjes, merret një vendim për propozimin ose jo të shpalljes së gjendjes së krizës kibernetike.
5. Në rastin kur vendoset të propozohet shpallja e gjendjes së krizës kibernetike, Autoriteti i dërgon Kryeministrit propozimin për shpalljen e krizës kibernetike dhe masat për zgjidhjen e situatës.
6. Kryeministri, me marrjen e propozimit nga Autoriteti, i propozon Këshillit të Ministrave shpalljen e gjendjes së krizës kibernetike.
7. Shpallja e gjendjes së krizës kibernetike bëhet me vendim të Këshillit të Ministrave.
8. Këshilli i Ministrave mund të vendosë zgjatjen e periudhës së gjendjes së krizës kibernetike, por jo më shumë se 30 ditë.

3. FAZA E PËRGJIGJES DHE MENAXHIMIT TË KRIZËS KIBERNETIKE

Faza e përgjigjes dhe menaxhimit të krizës kibernetike përfshin hapa të koordinuar dhe zbatimin e kundërmasave e *playbooks*-it për të minimizuar ndikimin, për të rikuperuar sistemet e prekura dhe për të siguruar vazhdimësinë e operacioneve kritike të infrastrukturës së informacionit, duke mundësuar kontrollin, kufizimin, neutralizimin, si dhe rikuperimin e pasojave të sulmit kibernetik të përshkallëzuar në krizë kibernetike, si dhe duke siguruar një koordinim institucional dhe komunikim të qartë. Faza e përgjigjes dhe menaxhimit të krizës kibernetike aktivizohet pas shpalljes zyrtare të gjendjes së krizës kibernetike me vendim të Këshillit të Ministrave.

3.1 Hapat për përgjigjen dhe menaxhimin ndaj krizës kibernetike

Hapat që ndiqen për përgjigjen dhe menaxhimin e krizës kibernetike janë, si më poshtë:

3.1.1 Aktivizimi i strukturave

3.1.1.1 Autoriteti Kombëtar për Sigurinë Kibernetike kërkon kalimin menjëherë në nivel gatishmërie të lartë të ekipit të përgjigjes ndaj incidenteve kibernetike pranë operatorit të sektorit/sektorëve të prekur nga incidenti kibernetik i përshkallëzuar në krizë kibernetike (CSIRT pranë operatorit), si dhe të kalojnë në gjendje emergjence kibernetike.

3.1.1.2 Autoriteti Kombëtar për Sigurinë Kibernetike kalon menjëherë në nivel gatishmërie të lartë Ekipin Kombëtar të Përgjigjes ndaj Incidenteve Kibernetike (CSIRT Kombëtar), si dhe kalon në gjendje emergjence kibernetike dhe nis procedurat e reagimit dhe koordinimit.

3.1.1.3 Autoriteti Kombëtar për Sigurinë Kibernetike ngre ekipin e përgjigjes ndaj emergjencave dhe krizës së sigurisë kibernetike (CERT), ku numri i ekspertëve dhe profilet e tyre vendoset mbi bazën e kompleksitetit të situatës, natyrës së sulmit, si dhe numrit të infrastrukturave të informacionit të prekura, sipas përcaktimeve të vendimit të Këshillit të Ministrave, për ngritjen, mënyrën e organizimit dhe funksionimit të ekipit të përgjigjes ndaj emergjencave dhe krizës së sigurisë kibernetike.

3.1.1.4 Në të gjitha rastet, komunikimi midis strukturave zhvillohet nëpërmjet kanaleve të sigurta të komunikimit, me qëllim shkëmbimin e informacionit teknik, njoftimin e aktorëve përgjegjës, si dhe koordinimin e masave urgjente.

3.1.2 Përditësimi i informacionit dhe vlerësimi i menjëhershëm i situatës

Autoriteti, në bashkëpunim me CERT-in mbledh dhe menaxhon të dhëna në kohë reale nga CSIRT-et pranë operatorëve si dhe nga CSIRT-et sektoriale, për sistemet dhe rrjetet e prekura, përmes të cilave realizohet analiza teknike e operacionale për shtrirjen e sulmit, ndikimin në shërbimet kritike, identifikimin e aktorëve të mundshëm, si dhe përcakton prioritetet për ndërhyrje. Autoriteti përditëson raportin e situatës çdo 24 (njëzet e katër) orë ose sipas nevojës.

3.1.3 Koordinimi ndërinstitucional dhe operacional

Autoriteti bashkërendon reagimin në nivel kombëtar dhe ndërkombëtar. Organizohen mbledhje të përditshme me:

a) CSIRT-et pranë operatorit dhe CSIRT-et sektoriale (p.sh. financa, energji, telekomunikacion, transport);

b) CERT-in;

c) Agjencitë e sigurisë (Policia e Shtetit, SHISH);

ç) Agjencitë partnere ndërkombëtare (p.sh. ENISA, EUROPOL EC3, NATO CCDCOE).

3.1.4 Përcaktimi, zbatimi dhe përditësimi i masave mbrojtëse e të kundërmasave kibernetike

Autoriteti përcakton e zbaton masat mbrojtëse të natyrës së përgjithshme dhe kundërmasat kibernetike për menaxhimin e krizës kibernetike, si dhe i përditëson ato sipas ecurisë së situatës.

3.1.5 Menaxhimi i komunikimit publik dhe transparenca

Autoriteti në koordinim me strukturën përgjegjëse për media dhe informim në varësi të Kryeministrit përgatit deklarata publike për të informuar qytetarët, duke shmangur panikun ose dezinformimin. Informacioni duhet të jetë i saktë dhe i bazuar mbi situatën aktuale, si dhe

nuk duhet të përmbajë informacion të ndjeshëm teknik. Menaxhimi i medias në një rast të krizës kibernetike do të bëhet sipas aneksit I, të kësaj procedure.

3.2 Mbledhja e informacionit dhe menaxhimi i të dhënave

Autoriteti, në bashkëpunim me CERT-in, mbledh, analizon e ruan të dhënat dhe informacionin, që mund të ndihmojnë në identifikimin, zbutjen dhe rikuperimin e pasojave të incidenteve në shkallë të gjerë. Elementet kyçe për mbledhjen e informacionit dhe menaxhimin e të dhënave janë, si vijon:

3.2.1 Mbledhja e të dhënave në kohë reale

- Përdoren sisteme të monitorimit të sigurisë për të mbledhur informacionin në kohë reale. Këto sisteme mund të identifikojnë aktivitete të dyshimta në rrjet dhe mund të regjistrojnë të dhënat e lidhura me incidentet e mundshme, si adresat IP të dyshimta, kërkesat anormale dhe lëvizjet e paautorizuara të të dhënave.
- Regjistrohen aktivitetet në sisteme dhe servera për të krijuar një gjurmë të plotë të asaj që ka ndodhur. Kjo mund të përfshijë log-et e sistemeve, log-et e rrjetit dhe regjistrat e ngjarjeve të sigurisë.

3.2.2 Klasifikimi dhe filtrimi i të dhënave

- Klasifikohet informacioni për të dalluar informacionin e rëndësishëm nga ai që nuk është i nevojshëm. Ky klasifikim përfshin ndarjen e të dhënave në kategori, si: të dhëna të ndjeshme, informacion për kërcënime, aktivitete të dyshimta etj.
- Filtrohen të dhënat, pasi jo të gjitha të dhënat janë të nevojshme për analizë. Filtrimi i të dhënave për të identifikuar informacionin më të rëndësishëm ndihmon në hetimin e incidentit kibernetik dhe mund të ndihmojë në gjetjen e burimit të sulmit.

3.2.3 Ruajtja dhe sigurimi i të dhënave

- Ruhen të dhënat e mbledhura në mënyrë të sigurt, në mënyrë që të mund të analizohen në të ardhmen dhe të përdoren si prova, nëse është e nevojshme. Ruajtja mund të përfshijë përdorimin e serverëve të veçantë të siguruar, duke përdorur enkriptimin dhe kontrollet e aksesit për të mbajtur të dhënat të papërshkueshme.
- Kryhet ruajtja e të dhënave me integritet të plotë. Të dhënat nuk duhet të manipulohen ose të modifikohen nga palë të treta pa autorizim. Përdorimi i metodave të enkriptimit dhe të kontrolleve të integritetit mund të ndihmojë në sigurimin e këtyre të dhënave.

3.2.4 Analiza e të dhënave dhe identifikimi i kërcënimeve

- Analizohen të dhënat e mbledhura dhe të ruajtura për të kuptuar natyrën dhe shkallën e incidentit kibernetik, si dhe për të identifikuar karakteristikat e dyshimta, për të kuptuar se si janë kompromentuar sistemet dhe rrjetet e informacionit.
- Përdoret *threat intelligence*, një proces që përfshin mbledhjen e informacionit të jashtëm për kërcënimet aktuale dhe përdorimin e tij për të përmirësuar reagimin ndaj incidentit kibernetik.

3.3 Burimet dhe kapacitetet kombëtare për përgjigjen dhe menaxhimin e krizës kibernetike në Shqipëri

Përballimi i krizave kibernetike kërkon koordinim të mirëfilltë dhe shfrytëzimin e burimeve dhe të kapaciteteve kombëtare në të gjithë sektorët. Ministritë, institucionet shtetërore, strukturat operacionale dhe aktorët joqeveritarë kanë kapacitete specifike, të cilat duhet të integrohen në një qasje gjithëpërfshirëse për të siguruar një përgjigje efektive ndaj krizave kibernetike.

3.3.1 Subjektet përgjegjëse

1. Këshilli i Ministrave;
2. Kryeministri;
3. Autoriteti Kombëtar i Sigurisë Kibernetike/CSIRT-i Kombëtar;
4. CERT/Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike;
5. CSIRT-i sektorial;
6. CSIRT-i pranë operatorit;
7. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale;

8. Policia e Shtetit.

3.3.2 Rolet dhe përgjegjësitë e subjekteve përgjegjëse për sigurinë kibernetike në fazën e përgjigjes

3.3.2.1 Këshilli i Ministrave, në cilësinë e organit kolegjial, me propozimin e Kryeministrit, merr vendim për:

a) shpalljen e gjendjes së krizës kibernetike për një periudhë 7-ditore.

b) zgjatjen e periudhës së gjendjes krizës kibernetike, por jo më shumë se 30 ditë.

3.3.2.2 Kryeministri i paraqet Këshillit të Ministrave propozimin për shpalljen e gjendjes së krizës kibernetike për një periudhë 7-ditore, si dhe zgjatjen e periudhës së gjendjes së krizës kibernetike, por jo më shumë se 30 ditë pas marrjes së propozimit për shpalljen e gjendjes së krizës kibernetike nga Autoriteti.

3.3.2.3 Autoriteti Kombëtar i Sigurisë Kibernetike/CSIRT-i Kombëtar është autoritet me kompetenca rregullatore, koordinuese, ekipi i përgjigjes ndaj incidenteve kibernetike dhe i krizës kibernetike dhe ushtron rolet e përgjegjësitë e mëposhtme:

a) I propozon Kryeministrit, në koordinim me institucionet e sigurisë dhe mbrojtjes, sikurse parashikohet në shkronjën "a", të nenit 11, të ligjit nr. 25/2024, "Për sigurinë kibernetike", shpalljen e gjendjes së krizës kibernetike dhe masat emergjente për zgjidhjen e situatës;

b) Thërret strukturën *ad-hoc* CERT;

c) Koordinon menaxhimin e krizës kibernetike;

ç) Nxjerr vendime me karakter të përgjithshëm ose merr masa mbrojtëse të natyrës së përgjithshme.

3.3.2.4 CERT – Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike është një strukturë *ad-hoc*, që vepron si linjë e parë e mbrojtjes për trajtimin e emergjencave dhe krizës së sigurisë kibernetike.

Detyrat kryesore:

a) Koordinimi dhe ndërhyrja e shpejtë për trajtimin e incidenteve kibernetike në shkallë të gjerë dhe krizave kibernetike;

b) Hartimi i planit të masave të emergjencës;

c) Menaxhimi dhe zgjidhja e emergjencës dhe krizës kibernetike;

ç) Ofrimi i asistencës në hartimin e rekomandimeve për të rikthyer në normalitet sistemet dhe rrjetet e informacionit në infrastrukturat e informacionit pas një incidenti në shkallë të gjerë dhe gjendjes së emergjencës dhe krizës kibernetike.

3.3.2.5 CSIRT-i sektorial, në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të sektorit përkatës:

a) raporton pranë CSIRT-it kombëtar incidentin kibernetik të ndodhur në infrastrukturat e informacionit të sektorit përkatës;

b) koordinon me CSIRT-et pranë operatorëve për t'iu përgjigjur situatës.

3.3.2.6 CSIRT-i pranë operatorit, në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të operatorit përkatës:

a) raporton incidentin e ndodhur në infrastrukturat e informacionit pranë operatorit të CSIRT-it kombëtar dhe CSIRT-it sektorial;

b) koordinon me CSIRT-in kombëtar dhe CSIRT-in sektorial për t'iu përgjigjur situatës.

3.3.2.7 Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, në cilësinë e institucionit përgjegjës për hartimin e politikave për mbrojtjen e të dhënave personale të individëve, monitoron zbatimin e legjislacionit përkatës në rastin e incidenteve në shkallë të gjerë dhe krizës kibernetike:

- Trajton, kontrollon dhe monitoron zbatimin e legjislacionit në fuqi për mbrojtjen e të dhënave personale.

3.3.2.8 Policia e Shtetit, në cilësinë e institucionit përgjegjës për hetimin e krimit kibernetik, në zbatim të legjislacionit penal kryen këto veprime:

a) Ndjek veprimet e nevojshme operacionale/procedurale, në kuadër të zbatimit të legjislacionit penal;

b) Bashkëpunon me CSIRT-in kombëtar dhe atë pranë operatorit për analizën dhe hetimin e incidentit kibernetik;

c) Realizon veprimet procedurale, në kuadër të zbatimit të legjislacionit penal.

4. FAZA E RIMËKËMBJES

4.1 Rimëkëmbja e shërbimeve pas krizës kibernetike

Rimëkëmbja pas krizës kibernetike përbën një proces të koordinuar, me qëllim rikthimin e shërbimeve dhe funksioneve kritike të infrastrukturës së informacionit në një gjendje të qëndrueshme. Ky proces siguron vazhdimësinë e operacioneve dhe rikthimin e sigurisë, duke minimizuar ndikimet afatgjata të krizës e duke përmirësuar gatishmërinë për incidente të ardhshme. Veprimet përfshijnë vlerësimin e dëmeve, rivendosjen graduale të sistemeve e të shërbimeve, monitorimin e vazhdueshëm për stabilitet e siguri gjatë rimëkëmbjes, si dhe dokumentimin e përvojës për të përmirësuar procedurat dhe *playbook*-et për menaxhimin e incidenteve të ardhshme.

4.2 Vlerësimi pas krizës dhe përmirësimi i qëndrueshmërisë

4.1.1 Pas stabilizimit të situatës, Autoriteti kalon në fazën e analizës retrospektive (*post-incident review*), që përfshin veprimet e mëposhtme:

a) Dokumenton të gjitha ngjarjet, reagimet dhe mësimet e nxjerra;

b) Analizon nëse protokollet e sigurisë ishin të mjaftueshme;

c) Përgatit raportin final të krizës kibernetike, që përfshin:

i. përshkrimin teknik të ngjarjes;

ii. vlerësimin e dëmit dhe kostove;

iii. masat e marra;

iv. rekomandimet për përmirësim.

4.1.2 Ky raport i dërgohet Kryeministrit dhe, sipas rastit, Komisionit Parlamentar të Sigurisë Kombëtare.

4.1.3 Në bazë të raportit final të krizës kibernetike, Autoriteti harton ose përditëson:

a) Procedurat e reagimit ndaj incidenteve kibernetike;

b) Politikat kombëtare të sigurisë digjitale;

c) Planet e trajnimit dhe ndërgjegjësimit për personelin publik dhe operatorët e infrastrukturave kritike.

ANEKSI I
MENAXHIMI I MEDIAVE NË NJË SITUATË KRIZE KIBERNETIKE

1. Rëndësia e menaxhimit të medias në rastin e një ngjarjeje kibernetike

CSIRT-i kombëtar, së bashku me institucionet ligjzbatuese, rregullatorët përkatës, ministritë e linjës dhe mediat luajnë një rol vendimtar në menaxhimin e kanaleve mediatike, në rastin e një krize kibernetike. Qytetarët duhet të marrin informacion të besueshëm, të përditësuar e të verifikuar.

Këto institucione duhet të ofrojnë informacion efektiv, që mund të shpëtojë jetë, të zvogëlojë shtrirjen e dëmtimeve dhe të shtyjë popullatën të marrë masat e nevojshme mbrojtëse. Në këto raste, komunikimi i nisur ka rezultuar të jetë më efektiv në përcaktimin e kufijve të një ngjarjeje kur ndahet me publikun, për të mos përhapur panik dhe për të përcjellë besueshmëri në popullatë.

2. Gjatë koordinimit me median mbahen në konsideratë elementet e mëposhtme:

a) **Kritika publike** – Incidentet kibernetike, që kanë jehonë në media, ndonjëherë çojnë në kritika që mund të vijnë edhe nga profesionistë kibernetikë, të cilët nuk janë domosdoshmërish të përfshirë në detaje, dhe nga palët e interesuara që punojnë në mënyrë rutinore me subjektin që dëmtohet;

b) **Identiteti i sulmuesit** – sulmuesi, në veçanti një shtet apo aktivist, kërkon vëmendjen dhe dukshmërinë e medias ndaj sulmit, si dhe ndikimin e tij në publik. Shpesh, një nga qëllimet e një sulmi është të bëjë "zhurmë" në media. Ndonjëherë, sulmuesi do të përpiqet të imitojë

dikë tjetër për të ngatërruar ose për të vështirësuar atribuimin. Identiteti i sulmuesit është tema më interesante për median, por është e rëndësishme të mbahet mend se identiteti i sulmuesit është zakonisht i paqartë dhe kërkon kohë gjatë një hetimi kibernetik për ta lidhur atë me një sulmues të caktuar;

c) **Dallimet ndërmjet infrastrukturave** – publiku nuk do të jetë gjithmonë në gjendje të bëjë dallimin ndërmjet infrastrukturës kritike dhe përgjegjësisë private kundrejt asaj kombëtare;

ç) **Siguria kibernetike është një gjuhë komplekse teknologjike**, që është shumë e pakuptueshme për publikun dhe ka boshllëqe në njohuri midis grupeve të ndryshme të popullsisë;

d) **Ngjarjet kibernetike kanë implikime politike** – deklarata të caktuara mund të ndikojnë në marrëdhëniet me vendet e tjera dhe veprimet pasuese;

dh) **Lloji dhe natyra e sulmit** zakonisht nuk ngjall interes mediatik, por më tepër pasojat e tij, megjithëse ka raste që krijojnë interes, kur ngjarja është veçanërisht e sofistikuar;

e) **Gjithçka është e lidhur** – Siguria kibernetike ndikon në të gjitha aspektet e jetës;

ë) **Sulmuesi kibernetik** mund të shkaktojë dëme fizike në terren (infrastruktura, shërbime, vazhdimësi operacionale, ndërprerje të transportit etj.) dhe dëmtim të ndërgjegjësimit (dëm ndaj qëndrueshmërisë kombëtare, pasiguri, dëmtim të aftësive parandaluese dhe dështim).

Audienca e synuar	**Qëllimet dhe objektivat e informacionit**
Popullsia që preket drejtpërdrejt nga ngjarja – klientët, subjektet, banorët e një zone të caktuar etj.	▪ Përshkruhet ngjarja dhe situata në mënyrë të besueshme; ▪ Jepen udhëzime; ▪ Sigurohet besimi tek entitetet e ndryshme dhe në aftësinë e tyre për të menaxhuar ngjarjen; ▪ Shmangen dezinformatat; ▪ Përcillen mesazhe uniforme nga të gjitha palët e përfshira; 🕮 Përshtaten mesazhet për popullatat e ndryshme të prekura nga ngjarja – niveli i ndërgjegjësimit, të kuptuarit teknologjik, gjuhët, dallimet kulturore, kanalet e ndryshme të komunikimit dhe ndikuesit.
Publiku i gjerë	▪ Përforcohet besimi i publikut; ▪ Sigurohet transparenca; ▪ Shmangen dezinformatat; 🕮 Përcillen mesazhe uniforme nga të gjitha palët e përfshira.
Komunikimet nga ofrues të ndryshëm shërbimi	▪ Përcillen mesazhe uniforme; ▪ Sigurohet transparenca; ▪ Të shmangen dezinformatat; Të përforcohet besimi në subjektin e ofruesit të shërbimit dhe në aftësinë për të menaxhuar ngjarjen.
Organet qeveritare	▪ Të përcjellin mesazhe uniforme; ▪ Të jenë transparent; ▪ Të shmangen dezinformatat; 🕮 Të përforcohet besimi aftësia për të menaxhuar ngjarjen.
Arena rajonale (kundërshtarët dhe armiqtë)	🕮 Parandalim/pengim i arritjeve të kundërshtarëve
Arena ndërkombëtare	▪ Konsolidimi i partneriteteve/koalicioneve kundër sulmuesit; 🕮 Delegjitimimi i sulmuesit dhe i sulmit.

Tabela 2: Përmbledhje e audiencës së synuar.

3. Sfidat për komunikimin e krizës

a) **Të ruhet raporti midis shpejtësisë dhe kujdesit në dhënien e informacionit** – ndërkohë që një raport i shpejtë, qoftë edhe i pjesshëm, drejton komunikimin, është e nevojshme t'i kushtohet vëmendje deklaratave që bëjnë pohime të forta, duke qenë se nuk janë të kolauduara e në vijimësi mund të rezultojnë të gabuara;

b) **Të mos zbulohet informacion kur nuk ka informacion** – në situata rreziku dhe krize, ajo që mund të shkaktojë panik është në fakt mungesa e informacionit;

c) **Të ruhet besimi i publikut tek autoritetet shtetërore dhe në hapësirën digjitale** – është e rëndësishme të sigurohet informacion gjithëpërfshirës dhe i besueshëm, të tregohet përkushtim dhe forcë në veprimet që ndërmerren për të menaxhuar ngjarjen e të demonstrohet se kriza mund të trajtohet. Gjithashtu, duhet të merren përgjegjësi, kur është e nevojshme, duke treguar udhëheqje dhe përmirësime apo mësime të nxjerra.

4. Rastet, në të cilat kryerja e një njoftimi, duhet të konsiderohet në mënyrë të favorshme:

a) Dëmtimi ose tentativa për dëmtim të infrastrukturave të informacionit që çojnë në dëmtimin e shërbimeve kritike për publikun, për shembull, transporti, furnizimi i mallrave, shërbimet shëndetësore, uji, energjia elektrike etj.;

b) Dëmtimi i një shërbimi që është me interes për publikun ose për një grup të caktuar individësh;

c) Dëmtimi i një infrastrukture të informacionit, që është e lidhur me infrastruktura të tjera dhe i rrezikon ato. Në këtë rast, është e nevojshme të paralajmërohen palët e interesit me infrastrukturën e informacionit të prekur;

ç) Përpjekje me efekt të gjerë në ekonomi, që nuk rezultojnë në dëmtime në terren dhe janë ndalur;

d) Rrjedhja e informacionit që është me interes dhe me rëndësi për publikun e gjerë ose për një grup të gjerë njerëzish;

dh) Ndërprerja e bazave të rëndësishme të të dhënave;

e) Një aktivitet që bën "zhurmë" ose që ka pasoja të gjera në publik;

ë) Dëmtimi i një shërbimi, një simboli qeveritar ose i një entiteti simbolik;

f) Financiar – një ngjarje e synuar ose e përhapur që i shkakton dëme të konsiderueshme një institucioni financiar, që mund të dëmtojë besimin e publikut në sistemin financiar shqiptar;

g) Shkaktimi i dëmeve të konsiderueshme ndaj infrastrukturave të informacionit që rezulton në një ndikim domethënës negativ në funksionimin e një numri të madh të infrastrukturave të informacionit, duke prekur vazhdimësinë e shërbimeve ose proceseve të tyre thelbësore.

gj) Një ngjarje që ndikon në mendësinë e njerëzve dhe/ose dezinformim, që ndikon në besimin e publikut, si rezultat i ngjarjes kibernetike. Kjo përfshin dëmtimin (vandalizimin) e një *website*-i të madh qendror ose i një tabele buletini me informacion jetik;

h) Përpjekje, me qëllim për të dëmtuar sigurinë publike dhe shoqërinë ose një ngjarje, që në mënyrë indirekte ose direkte, ka rezultuar në dëmtim personal të individit.

5. Përballja me dezinformimin dhe lajmet e rreme

Lajmet e rreme dhe dezinformatat janë një problem global. Gjatë një ngjarjeje, rekomandohet të trajtohet fenomeni shpejt dhe në mënyrë efektive, duke përdorur mjetet e mëposhtme:

a) Monitorimi i informacioneve të rreme përmes sistemeve për monitorimin e diskutimit në internet dhe/ose përdorimit të një personi nga infrastruktura, që do të kërkojë në mënyrë aktive kanalet sociale. Është e mundur të krijohet një qendër komandimi për të monitoruar dhe dhënë përgjigje ose për të përdorur dhomat ekzistuese të operacioneve;

b) Marrja e një vendimi për llojin e përmbajtjes që do të trajtohet - çfarë dezinformimi është i rëndësishëm, sipas disa kritereve, çfarë e shkakton mosbesimin e publikut, çfarë është mashtruese dhe mund të shkaktojë dëm;

c) Përhapja e informacionit të besueshëm në mënyrë të vazhdueshme dhe të shpejtë për të parandaluar krijimin e një vakumi që do të mbushet me teori e gënjeshtra;

ç) Vendosja e autoritetit dhe besimit në informacionin dhe në kanalet e institucionit, duke përdorur ekspertë vendas ose të jashtëm, video, imazhe dhe tekste;

d) Dhënia e shembujve duke përdorur vetëmashtrimin – tregohet se çfarë është e gabuar dhe pse për të hedhur poshtë pretendimin; i bëhet thirrje publikut që të shpërndajë informacion të saktë. Për shembull, bëhet një foto e lajmeve të rreme dhe shtohet një etiketë që lexon "Mashtrim /Paralajmërim! Lajme të rreme!"). Shkruhet një artikull mbi këtë temë dhe shfaqet informacioni i rremë;

dh) Kur media përhap lajme të rreme ose dezinformata është e rëndësishme t'i thuhet atyre qartë se e kanë gabim;

e) Përdorimi i njerëzve të jashtëm që do të veprojnë dhe do t'u përgjigjen informacioneve të rreme;

ë) Evidentimi i rasteve specifike në media për të rritur ndërgjegjësimin e publikut për fenomenin, shpjegohet fenomeni, çfarë është informacioni i rremë dhe si të përgënjeshtrohet. Inkurajohet të menduarit kritik.