VENDIM
Nr. 126, datë 30.7.2020

MBI MIRATIMIN E "RREGULLORES PËR SIGURINË KIBERNETIKE TË INFRASTRUKTURAVE KRITIKE NË SEKTORIN E ENERGJISË ELEKTRIKE"

Në mbështetje të nenit 18, të ligjit nr. 43/2015, "Për sektorin e energjisë elektrike", i ndryshuar, të ligjit nr. 2/2017, "Për sigurinë kibernetike", VKM-së nr. 553, datë 15.7.2020, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit", si dhe të nenieve 15 dhe 26 të "Rregullores së organizimit, funksionimit dhe procedurave të ERE-s", miratuar me vendimin e Bordit të ERE-s nr. 96, 17.6.2016, Bordi i Entit Rregullator të Energjisë (ERE), në mbledhjen e tij të datës 30.7.2020, mbasi shqyrtoi relacionin nr. 92/3 prot., datë 23.7.2020, të përgatitur nga grupi i punës, mbi miratimin e "Rregullores për sigurinë kibernetike të infrastrukturave kritike në sektorin e energjisë elektrike",

konstatoi se:

- Bordi i ERE-s, me vendimin nr. 235, datë 20.12.2019, vendosi mbi fillimin e procedurës për miratimin e "Strategjisë për infrastrukturat kritike në sektorin e energjisë elektrike".

- Lidhur me këtë vendim të Bordit të ERE-s, me shkresën nr. 886, datë 31.12.2019, janë njoftuar Ministria e Infrastrukturës dhe Energjisë, Autoriteti i Konkurrencës, OSHEE sh.a., OST sh.a., KESH sh.a. dhe Sekretariati i Komunitetit të Energjisë Elektrike, dhe janë ftuar të japin komentet apo sugjerimet e tyre në lidhje me draftin për të cilin filloi procedura në ERE. Gjithashtu, me shkresën nr. 83/1, datë 21.1.2020, u njoftuan palët e interesit për organizimin e një seance dëgjimore me qëllim diskutimin mbi draftin e "Strategjisë për infrastrukturat kritike në sektorin e energjisë elektrike".

- Me shkresën nr. 758, datë 20.11.2019, ERE i ka propozuar "Ministrisë së Infrastrukturës dhe Energjisë", duke bërë me dije "Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike", si dhe KESH sh.a., përditësimin e "Listës së infrastrukturave kritike të informacionit", për të përfshirë në listën e këtyre infrastrukturave edhe infrastrukturat e kompanisë publike të prodhimit.

- Në vijim të sa më sipër, Ministria e Infrastrukturës dhe Energjisë me shkresën nr. 144/2, datë 28.4.2020, konfirmon në lidhje me marrjen dijeni të fillimit të procedurës për miratimin e "Strategjisë për infrastrukturat kritike në sektorin e energjisë elektrike", si dhe informon se **OSHEE sh.a.** propozon që pjesë e infrastrukturës kritike të jenë:

- Sistemi i faturimit të OSHEE sh.a.;
- Sistemi i leximit të matësve (Mobiread);
- Sistemi financiar (SAP);
- Sistemi i monitorimit të nënstacioneve dhe kabinave (SCADA).

OST sh.a. propozon që pjesë e infrastrukturës kritike të jetë:

- Sistemi i monitorimit dhe komandimit (SCADA);

KESH sh.a. propozon që pjesë e infrastrukturës kritike të jenë:

- ABB Symphony SCADA system;
- Rrjeti i transmetimit të të dhënave (komunikimit) i KESH sh.a. (Tiranë – HEC Vau i Dejës, Tiranë – HEC Fierzë, Tiranë – HEC Koman);
- Draftstrategjia iu dërgua me email USAID-it dhe ACER-së (Agjencisë së Rregullatorëve Evropiane), si dhe iu janë kërkuar komente në lidhje me këtë "Draftstrategji për infrastrukturat kritike në sektorin e energjisë elektrike".

- Në vijim, me shkresën nr. 935 prot., datë 26.6.2020, drafti i "Rregullores për sigurinë kibernetike të infrastrukturave kritike në sektorin e energjisë elektrike" iu dërgua për komente dhe sugjerime edhe "Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike".

- Duke qenë se pritet që AKCESK-ja, do të miratojë "Strategjinë kombëtare të sigurisë kibernetike 2020–2025", e cila përfshin dhe operatorët e sistemit energjetik në vendin tonë, miratimi nga ERE i një strategjie të tillë do të sillte mbivendosje të dy strategjive dhe do të krijonte konfuzion se cila nga strategjitë e miratuara do të implementohet në sektorin e energjisë elektrike.

- ERE vlerëson se në zbatim të përcaktimeve ligjore duhet të miratojë rregulloren përkatëse për sigurinë kibernetike të infrastrukturave kritike në sektorin e energjisë elektrike.

- Komentet dhe opinionet e palëve të interesuara dhe konsulentëve, janë marrë parasysh dhe janë reflektuar në rregullore duke bërë përshtatjen e nevojshme me aktet ligjore e nënligjore në fuqi.

Për gjithë sa më sipër cituar, Bordi i ERE-s

VENDOSI:

1. Miratimin e "Rregullores për sigurinë kibernetike të infrastrukturave kritike në sektorin e energjisë elektrike" (bashkëlidhur).

2. Drejtoria Juridike dhe Zgjidhjes së Mosmarrëveshjeve, të njoftojë palët e interesit për vendimin e Bordit të ERE-s.

Ky vendim hyn në fuqi menjëherë.

Për këtë vendim mund të kërkohet rishikim brenda 7 ditëve kalendarike si dhe mund të bëhet ankim në Gjykatën Administrative Tiranë, brenda 30 ditëve kalendarike nga dita e publikimit në Fletoren Zyrtare.

Ky vendim botohet në Fletoren Zyrtare.

KRYETAR
Petrit Ahmeti

RREGULLORE
PËR SIGURINË KIBERNETIKE TË INFRASTRUKTURAVE KRITIKE NË SEKTORIN E ENERGJISË ELEKTRIKE

Neni 1
Autoriteti

Enti Rregullator i Energjisë ka ndër objektivat e përcaktuar në nenin 18, të ligjit nr. 43/2015 "Për sektorin e energjisë elektrike", i ndryshuar, promovimin dhe krijimin e një tregu të brendshëm konkurrues të sigurt dhe miqësor ndaj mjedisit për të gjithë klientët dhe furnizuesit, duke siguruar kushtet e duhura për funksionimin e sigurt dhe të qëndrueshëm të rrjeteve të energjisë elektrike, në bashkëpunim të ngushtë me Komunitetin e Energjisë dhe autoritetet rregullatore të vendeve të tjera. Neni 26, i ligjit nr. 43/2015, gjithashtu, përcakton se, sistemi i energjisë elektrike operon si një sistem i integruar me procese të vazhdueshme prodhimi, transmetimi, shpërndarjeje dhe konsumi të energjisë elektrike. Bazuar në sa më sipër, ERE konsideron sigurinë kibernetike në sektorin e energjisë elektrike si element themelor për ruajtjen e sigurisë dhe integritetit të sistemit elektroenergjetik shqiptar.

Neni 2

Qëllimi

Qëllimi i kësaj rregulloreje është të përcaktojë rregullat dhe masat që duhet të ndërmerren nga subjektet e licencuara nga ERE në sektorin e energjisë elektrike, të cilët kanë përgjegjësi të garantojnë sigurinë kibernetike në infrastrukturat kritike që zotërojnë dhe operojnë. Garantimi i sigurisë kibernetike në sistemin elektroenergjetik siguron furnizimin e pandërprerë me energji elektrike të konsumatorëve në vendin tonë.

Neni 3
Objekti

Kjo rregullore përcakton detyrimin e operatorëve që zotërojnë ose operojnë infrastrukturat kritike në sektorin e energjisë elektrike për të vendosur dhe zbatuar masat e duhura gjatë projektimit, instalimit dhe funksionimit të rrjetit ose pajisjeve të përdorura prej tyre, në mënyrë që të garantojnë sigurinë, disponueshmërinë, integritetin dhe funksionimin e qëndrueshëm të sistemit elektroenergjetik. Operatorët duhet të paraqesin pranë ERE-s, sipas shtojcës nr. 2 dhe shtojcës nr. 3, raporte për çdo ndërhyrje të paplanifikuar, cenim ose incident në fushën e sigurisë, disponueshmërisë dhe integritetit të rrjeteve të tyre të komunikimit elektronik, si dhe çdo ndërhyrje, dëmtim që ka ndikim në funksionimin e rrjeteve dhe/ose të statusit të tyre të shërbimit.

Neni 4
Përcaktimi i termave

Termat e përdorur në këtë rregullore do të kenë kuptimin e mëposhtëm. Çdo term tjetër i përdorur në rregullore do të ketë kuptimin e përcaktuar në ligjin nr. 43/2015 "Për sektorin e energjisë elektrike", i ndryshuar, ose në ligjin nr. 2 /2017 "Për sigurinë kibernetike".

1. "CSIRT" – është ekipi i përgjigjes ndaj incidenteve të sigurisë kompjuterike.
2. "CSIRT sektorial" – është ekipi/ personi përgjegjës ndaj incidenteve të sigurisë kibernetike, në strukturën e një operatori që administron infrastruktura kritike dhe të rëndësishme të informacionit.
3. "Hapësirë kibernetike" – është mjedisi digjital i aftë të krijojë, të procesojë dhe të shkëmbejë informacionin e krijuar nga sistemet, shërbimet e shoqërisë së informacionit, si dhe rrjetet e komunikimit elektronik.
4. "Incident i sigurisë kibernetike" - është një ngjarje e sigurisë kibernetike, gjatë së cilës shkaktohet cenimi i sigurisë së shërbimeve ose sistemeve të informacionit e të rrjeteve të komunikimit dhe sjell një efekt real negativ.
5. "Infrastrukturë kritike e informacionit" – është tërësia e rrjeteve dhe sistemeve të informacionit, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë dhe/ose mirëqenien ekonomike të qytetarëve dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë.
6. "Operator i infrastrukturës kritike të informacionit" – është një person juridik, publik ose privat, që administron infrastrukturën kritike të informacionit dhe operon në sektorin e energjisë elektrike OST sh.a., OSHEE sh.a. dhe KESH sh.a..
7. "Rrezik i sigurisë kibernetike" – është një rrethanë ose një ngjarje, e identifikueshme në mënyrë të arsyeshme, e cila mund të shkaktojë cenimin e sigurisë së shërbimeve ose sistemeve të informacionit dhe të rrjeteve të komunikimit.
8. "Siguria e informacionit" – është sigurimi i konfidencialitetit, integritetit dhe disponueshmërisë së informacionit.

9. “Siguria kibernetike” - është tërësia e mjeteve ligjore, organizative, teknike dhe edukative, me qëllim mbrojtjen e hapësirës kibernetike.

10. “SKI” – janë sistemet e komunikimit dhe informacionit.

11. “AKCESK” – është Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike.

Neni 5

Rregulla të përgjithshme dhe parime bazë

1. Rregullorja për sigurinë kibernetike në infrastrukturat kritike në sektorin e energjisë elektrike është hartuar bazuar në nenin 18, të ligjit nr. 43/2015 “Për sektorin e energjisë elektrike” i ndryshuar, ligjit nr.2/2017 “Për sigurinë kibernetike” dhe VKM nr. 553, datë 15.7.2020, “Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit”, duke marrë parasysh që:

a) Qëllimi i ligjit nr. 43/2015 “Për sektorin e energjisë elektrike”, i ndryshuar, është që përmes kuadrit teknik dhe ligjor të sigurohet furnizim i sigurt dhe i qëndrueshëm me energji elektrike i konsumatorëve, në përputhje me zhvillimet teknologjike. Ligji nr. 2/2017 “Për sigurinë kibernetike” ka për qëllim arritjen e një niveli të lartë mbrojtjeje të sigurisë kibernetike dhe gatishmërinë ndaj sulmeve kibernetike, duke përcaktuar masat e sigurisë, të drejtat, detyrimet, si dhe bashkëpunimin e ndërsjellë ndërmjet operatorëve të infrastrukturave kritike përfshirë në sektorin energjetik, përmes të cilave sigurohen shërbimet e licencuara.

b) Operatori i infrastrukturave kritike në sektorin e energjisë elektrike duhet të ndërmarrë masat e duhura proporcionale, me kosto efektive, teknike dhe organizative për garantimin e sigurisë rrjetit për të menaxhuar, adresuar dhe trajtuar në mënyrën e duhur rreziqet që paraqiten për sigurinë e rrjeteve dhe të informacionit që ata menaxhojnë në përmbushje të aktiviteteve të tyre dhe duke respektuar rolet e tyre.

2. Ndër të tjera kjo rregullore shërben si dokument mbështetës për operatorët e infrastrukturave kritike në përputhje me kërkesat e ligjit nr. 2/2017 “Për sigurinë kibernetike”. Për infrastrukturat kritike dhe akteve nënligjore në zbatim të tij, si dhe vendos procese për të ndihmuar OIKI-në të demonstrojnë dhe të vërtetojnë se ata po menaxhojnë rreziqet e sigurisë kibernetike në lidhje me shërbimet e ofruara. Këto procese përfshijnë kryesisht:

a) Vetëvlerësimi nga OIKI-ja

OIKI-ja do të paraqesë vetëvlerësimin e tij në ERE bazuar në “Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë (miratuar me urdhër nr. 22, datë 26.4.2018, të AKCESK-së). Ky vetëvlerësim do të përmbajë një informacioni të detajuar dhe të plotë (duke përfshirë metodologjinë që ka përdorur për të realizuar vetëvlerësimin, mënyrën se si e ka aplikuar këtë metodologji rezultatet e vetëvlerësimit të cilat duhet të përfshijnë identifikimin e riskut si dhe procesin e zvogëlimit të riskut) të çdo rreziku domethënës të identifikuara dhe çdo propozim fillestar për trajtimin e rrezikut përfshirë deklarim për rezultatin e nxjerrë duke identifikuar atë si “Jo e arritur” ose “Pjesërisht e arritur” dhe “e Arritur”.

Ky informacion duhet të dorëzohet duke përdorur modelin e raportimit të vetëvlerësimit, i cili gjendet në shtojcën. nr. 1.

Pasi të paraqitet informacioni në ERE, nëse ERE e gjykon të arsyeshme, mund të hyjë në vlerësime dhe të kërkoj informacione të mëtejshme për çështjet e raportuar për të realizuar vlerësimet përkatëse. Kjo mund të përfshijë një kërkesë për sqarime të mëtejshme mbi rezultatet e vetëvlerësimit që konsiderohen si “Jo e arritur” ose “Pjesërisht e arritur”. Nëse informacioni që është dërguar në ERE është i paqartë ERE mund të kërkojë sqarime nga OIKI-ja.

OIKI-ja në çdo kohë mund të kërkojë që të konsultohet me ERE sa më shpejt të jetë e mundur nëse nuk është i sigurt për çështjet objekt raportimi. Pasi OIKI-ja të ketë përfunduar vetëvlerësimin e tyre, OIKI-ja duhet të marrin në konsideratë fushat për përmirësim.

Në vetëvlerësimin fillestar që do të realizohet nga OIKI-ja, qëllimi kryesor është kryerja e një vetëvlerësim objektiv dhe bazuar në rezultatet e vetëvlerësimit, OIKI-ja duhet të zhvillojnë një plan përmirësimi, atje ku ato janë të nevojshme ose sipas prioriteteve të përcaktuara nga ERE. Çdo vlerësim sipas statusit respektiv i arritur ose jo do të shoqërohet me shpjegimet përkatëse për çdo konkluzion. ERE mund të kërkojë që raportet e vetëvlerësimeve të përgatitura nga OIKI-ja të jenë të audituara.

b) Identifikimi dhe hartimi i planit të masave duke pasur parasysh rreziqet e mundëshme dhe të identifikuara

Pas procesit për paraqitjen e vetëvlerësimit të përcaktuar më lart, OIKI-ja duhet të propozojnë planet e tyre të masave tek autoritetet kompetente. OIKI-ja mund të kërkojë bashkëpunim me ERE siç përcaktohet më lart.

Planet e masave bazohen në vetëvlerësimet e OIKI-së duke identifikuar rreziqet në përputhje me procesin e tyre të menaxhimit të riskut dhe metodologjinë e riskut. Plani i përmirësimit duhet të përcaktojë planet e veprimit të sigurisë kibernetike që OIKI-ja synon të marrë atje ku rreziku është vlerësuar më i lartë duke konsideruar nivelet e tolerancës ndaj rrezikut. Planet e masave mund të përfshijnë ndër të tjera masat afatshkurtra ose masa strategjike afatgjata, për të cilat duhet të rivlerësohet buxheti i OIKI-së përmes planifikimit të duhur të biznesit. ERE, rast pas rasti, mund të kërkojë rishikimin e planit të masave nga OIKI-ja në mënyrë që t'i ndihmojë ata në prioritarizimin dhe planifikimin e mbrojtjes nga rreziku kibernetik.

c) Identifikimi dhe rishikimi i planeve të investimeve, të cilat duhet të marrin në konsideratë nevojën për të zvogëluar rreziqet e identifikuara në pikën (2.b)

OIKI-ja duhet të zhvillojë një sistem të menaxhimit të sigurisë së informacionit, për të menaxhuar në mënyrën e duhur rreziqet kibernetike, në çdo hallkë të sistemit të furnizimit. Ky sistem do të sigurohet brenda afatit të përcaktuar nga ERE sipas analizës dhe propozimit të OIKI-së, dhe mund të përfshijë ndër të tjera angazhimin e ekspertëve në fushën e sigurisë së teknologjisë së informacionit si dhe trajnime të ndryshme. Afatet kohore për iniciativat dhe kundërmasat e sigurisë kibernetike do të jenë pjesë e plani të përmirësimit. Prioriteti i masave të sigurisë së rrjeteve për rreziqet e larta duhet të bazohet në raportin e vetëvlerësimit rast pas rasti.

3. Pas paraqitjes së planit të parë të vetëvlerësimit dhe përmirësimit, ERE mund të kryejë monitorime në OIKI dhe në vijim të rezultateve të monitorimit do të paraqesë me rekomandimet përkatëse.

Neni 6

Detyrime të operatorëve të infrastrukturave kritike

1. Për qëllime të kësaj rregulloreje detyrat e operatorëve të infrastrukturave kritike në sektorin energjetik përfshijnë:

a) OIKI-ja duhet të marrë masat teknike dhe organizative për të menaxhuar rreziqet që mund t'i shfaqen e që lidhen me sigurinë e rrjetit dhe të sistemeve të informacionit në të cilat mbështetet shërbimi i licencuar nga ERE, me qëllim sigurimin e vazhdimësisë së shërbimeve objekt licencimi, referuar "Rregullores mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë" (miratuar me urdhër nr. 22, datë 26.4.2018, të AKCESK-së);

b) OIKI-ja duhet të marrë masa për të parandaluar dhe minimizuar ndikimin e incidenteve që ndikojnë në sigurinë e rrjetit dhe sistemeve të informacionit të përdorura për sigurimin e shërbimit

për të cilin janë licencuar nga ERE, me qëllim të sigurimit të vazhdimësisë së këtyre shërbimeve. Kategoritë e incidenteve kibernetike përcaktohen sipas "Rregullores për kategoritë e incidenteve kibernetike, si dhe formatin e elementët e raportimit (miratuar me urdhrin nr. 62, datë 10.9.2018, të AKCESK-së);

c) OIKI-ja do të jenë përgjegjës për zbatimin e masave që garantojnë sigurinë kibernetike nga palët e treta që ofrojnë shërbime ose produkte të infrastrukturës kritike. Operatorët e rrjetit OST sh.a. dhe OSSH sh.a. do të jenë, gjithashtu, përgjegjës për zbatimin e masave të sigurisë kibernetike nga përdoruesit respektivë të rrjetit;

d) OIKI-ja ka për detyrë për të njoftuar incidentet pranë ERE-s dhe Autoritetit të përcaktuar në përputhje me ligjin nr. 2 /2017 "Për sigurinë kibernetike". Njoftimi do të kryhet për çdo incident i cili ka një ndikim të rëndësishëm në vazhdimësinë e shërbimit dhe veprimtarisë së licencuar.

2. Në përputhje me përcaktimet e pikës 1, të këtij neni, OIKI, do të raportojë periodikisht një herë në gjashtë muaj, brenda muajit janar dhe korrik për 6-mujorin paraardhës, sipas shtojcës 1, të kësaj rregulloreje, për çështjet që lidhen me zbatimin e germave "a", "b" dhe "c", të pikës 1, të këtij neni, dhe në çdo rast tjetër do të njoftojë menjëherë dhe jo më vonë se 4 orë nga momenti i zbulimit të incidentit të sigurisë të identifikuar sipas germës "d", të pikës 1, të këtij neni.

3. Faktorët kryesorë për vlerësimin e realizimit nga operatori të detyrave sipas kësaj rregulloreje do të monitorohen nga ERE. Në çdo rast, ERE do të vlerësojë:

- nëse janë zbatuar apo jo masa të përshtatshme dhe propocionale të sigurisë kibernetike sipas detyrave që ka OIKI-ja;
- nëse incidentet i janë njoftuar ERE-s.

Frekuenca e ndodhjes së një incidenti sipas germës "d", pika 1, të nenit 6, në vetvete nuk do të thotë se detyrimisht ka pasur një dështim nga një operator për të përmbushur detyrat e tij të sigurisë.

Brenda 30 ditëve nga ndodhja e një incidenti në infrastrukturat kritike, OIKI-ja duhet të paraqesë një raport të përgjithshëm për ERE-n. Brenda 90 ditëve nga ndodhja e incidentit në infrastrukturat kritike, OIKI-ja duhet të paraqesë në ERE një raport të detajuar të hetimit të incidentit.

ERE, gjithashtu, mund të kërkojë OIKI-së të dorëzojnë pranë ERE-s raporte të audituar në lidhje me hetimin e një incidenti të sigurisë kibernetike.

Neni 6/1

Detyrime të tjera

Operatorët e infrastrukturave kritike në sektorin e energjisë veç detyrave të përcaktuara në nenin 6, të kësaj rregullore, do të marrin masa dhe për zbatimin e përcaktimeve të parashtruara më poshtë në këtë nen:

1. Zbatimin e masave të plota organizative dhe teknike të sigurisë kibernetike në sistemet e komunikimit dhe të informacionit (SKI) nëpërmjet:

a) mbrojtjes së infrastrukturave kritike të informacionit për garantimin e shërbimeve;

b) menaxhimit të aseteve të teknologjisë së komunikimit dhe informacionit;

c) kontrollit të vijueshëm të masave të sigurisë;

d) vlerësimit të vijueshëm të masave të sigurisë;

e) reflektimit të kërkesave të sigurisë në projektet e reja të sistemeve të komunikimit dhe informacionit;

f) zbatimit të teknologjive mbrojtëse;

2. Rritjen e përgjegjësisë së operatorëve të infrastrukturave kritike për sigurinë kibernetike nëpërmjet:

a) hartimit dhe zbatimit të rregullave dhe procedurave të sakta për strukturat përgjegjëse për sigurinë kibernetike në OIKI;

b) hartimit dhe zbatimin e formateve dhe mënyrave të raportimit të sulmeve kibernetike për strukturat përgjegjëse për sigurinë kibernetike në OIKI;

c) zhvillimit të kapaciteteve dhe strukturave të dedikuara për sigurinë kibernetike;

d) koordinimit ndërmjet strukturave për reagimin ndaj sulmeve kibernetike;

e) shkëmbimit të informacionit për sigurinë kibernetike;

3. Zhvillimin e nivelit dhe aftësive të specialistëve të sigurisë kibernetike dhe të përdoruesve të SKI-ve nëpërmjet:

a) rekrutimit dhe caktimit në detyrë të specialistëve për sigurinë e kibernetike;

b) trajnimit të vijueshëm të specialistëve, promovimi dhe certifikimi i tyre;

c) konceptimit të trajnimit si një fushë komplekse ku të përfshihet reagimi ndaj incidenteve, testimet penetruese në sisteme, menaxhimi rrezikut, analizat e kërcënimit, mënyrat paralajmëruese;

d) trajtimit të mbrojtjes kibernetike në programet e trajnimit të stafit përgjegjës të operatorëve të infrastrukturave kritike.

4. Rritjes së bashkëpunimit ndërmjet operatorëve të infrastrukturave kritike në fushën e energjisë elektrike për sa i përket sigurisë kibernetike nëpërmjet:

a) bashkëpunimit në bazë të përcaktimeve të politikës së sigurisë së mbrojtjes kibernetike të Republikës së Shqipërisë;

b) detyrimeve të ligjit nr. 2/2017 "Për sigurinë kibernetike";

c) pjesëmarrje në trajnime për mbrojtjen kibernetike.

d) shkëmbimit të informacionit të ndërsjellë që lidhet me sigurinë kibernetike ndërmjet OIKI-së.

Neni 7

CSIRT-ja sektoriale

Operatorët e infrastrukturës kritike të informacionit në sektorin e energjisë elektrike do të përcaktojnë personat përgjegjës për koordinimin, ndjekjen dhe zbatimin e masave për sigurinë kibernetike. Këta përfaqësues do të jenë pjesë e ekipit të përgjigjes ndaj incidenteve të sigurisë kompjuterike (CSIRT-së sektoriale). Përcaktimi i personave përgjegjës për sigurinë kibernetike duhet të bëhet brenda 3 muajve pas hyrjes në fuqi të kësaj rregulloreje. Gjithashtu, operatorët e infrastrukturës kritike të informacionit në sektorin e energjisë elektrike do të hartojnë rregullat dhe mënyrën e funksionimit të CSIRT-së sektoriale, duke iu referuar edhe "Udhëzimit për metodologjinë e organizimit dhe funksionimit të CSIRT-eve në nivel kombëtar (neni 7, pika 3, e ligjit nr. 2/2017 "Për sigurinë kibernetike").

Neni 8

Raportimi

Operatorët e infrastrukturës kritike të informacionit në sektorin e energjisë elektrike do të raportojnë menjëherë dhe jo më vonë se 4 orë nga momenti i zbulimit të incidentit të sigurisë për çdo rast që përbën një shkelje/ndërhyrje, e cila ka cenuar sigurinë kibernetike të infrastrukturave kritike që i licencuari zotëron ose operon, si dhe të çdo shërbimi tjetër që operatori ka në përdorim nga palë të treta.

ERE, me paraqitjen e informacioneve nga të licencuarit në rast të incidenteve të raportuara, do të shqyrtojë rastin e raportuar me të licencuarin për të vlerësuar:

- nëse incidenti ka ndodhur për shkak të veprimeve apo mosveprimeve të operatorit;

- mbi nevojën për rishikimin e akteve rregullatore apo nevojën për mbështetje nga institucionet e tjera ligj zbatuese për veprimet e propozuara me qëllim shmangien, parandalimin apo uljen e numrit të incidenteve.

Në çdo rast ERE mund të kërkojë informacion të detajuar nga OIKI-ja për të mbështetur çdo vlerësim mbi pajtueshmërinë e veprimeve të të licencuarit me rregullat që lidhen me sigurinë e infrastrukturave kritike.

Nëse ERE konkludon se bashkëpunimi me OIKI-në nuk ka funksionuar ose është e qartë se nuk janë marrë masat e duhura për shmangien e incidenteve në infrastrukturat kritike, ERE do të njoftojë operatorin për dështimet e identifikuara. ERE mund të vendosë afate kohore për të korrigjuar dështimet e evidentuara në OIKI.

Neni 9
Penalitetet

Në rast se i licencuari nuk vepron në përputhje me planin e masave, ndaj tij zbatohen sanksione në përputhje me nenin 107, të ligjit nr. 43/2015 "Për sektorin e energjisë elektrike", si dhe "Rregulloren për procedurat e vendosjes dhe reduktimit të gjobave", miratuar me vendimin e Bordit të ERE-s.

Neni 10
Certifikim me standardin e sigurisë ISO 27001

Operatorët e infrastrukturave kritike në sektorin e energjisë elektrike të pajisen me certifikimin me standardin e sigurisë ISO 27001 brenda 18 muajve nga hyrja në fuqi e kësaj rregulloreje.

Neni 11
Dispozita përfundimtare

Kjo rregullore hyn në fuqi pas miratimit dhe publikimit të vendimit të Bordit të ERE në fletoren zyrtare.

SHTOJCË 1
RAPORTI I VETËVLERËSIMIT MBI MBROJTJEN E INFRASTRUKTURAVE KRITIKE DHE MENAXHIMI I RISKUT

Operatori bazuar në "Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë (miratuar me urdhrin nr. 22, datë 26.4.2018, të AKCESK-së)", do të raportojë mbi:

Masat organizative, të:

a) menaxhimit të sigurisë së informacionit,
b) menaxhimit të rrezikut,
c) politikave të sigurisë,
ç) sigurisë organizative,
d) kërkesave të sigurisë për palët e treta,
dh) menaxhimit të aseteve,
e) sigurisë së burimeve njerëzore dhe aksesit të personave,
ë) ngjarjeve të sigurisë dhe menaxhimit të incidenteve të sigurisë kibernetike,
f) menaxhimit të vazhdimësisë së punës,

g) kontrollit dhe auditit,

Masat teknike, të:

a) sigurisë fizike,

b) mbrojtjes së integritetit të rrjeteve të komunikimit,

c) verifikimit të identitetit të përdoruesve,

ç) menaxhimit për autorizimin e aksesit,

d) veprimtarisë së administratorëve dhe të përdoruesve,

dh) zbulimit të ngjarjeve të sigurisë kibernetike,

e) mjeteve të gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike,

ë) sigurisë së aplikacioneve,

f) të pajisjeve kriptografike,

g) sigurisë së sistemeve industriale.

SHTOJCË 2

Formulari për raportimin e një incidenti të sigurisë dhe/ose cenimit të integritetit	
Informacion kontakti	*Emri i sipërmarrësit:*
	Emri dhe mbiemri i personit të ngarkuar me eliminimin e incidenteve të sigurisë dhe/ose cenimit të integritetit:
	Pozicioni i punës:
	Adresa:
	Telefon, e-mail:
Përshkrimi i incidentit të sigurisë dhe/ose cenimit të integritetit	*Lloji:*
	Përcaktimi se cilat rrjete, sisteme ose shërbime preken nga incidenti i sigurisë:
	Koha e ndodhjes dhe kohëzgjatja:
	Informacion rreth shkakut fillestar ose shkaqeve:
	Përshkrimin e incidentit (përcaktoni të dhënat në mënyrë sa më të detajuar):
	Numri i përafërt i përdoruesve të prekur nga incidenti i sigurisë ose cenimi i integritetit ose përqindja e tyre (%) nga përdoruesit total të rrjetit dhe/ose shërbimit:
	Zona gjeografike e prekur nga incidenti i sigurisë dhe/ose cenimi i integritetit (km²):
	Burimet e prekura
	Pasojat:
Menaxhimi i incidentit të sigurisë dhe/ose cenimit të integritetit	*Veprimet e ndërmarra (të planifikuara për t'u ndërmarrë) për të eliminuar incidentin e sigurisë dhe për të reduktuar pasojat e tij:*
	Masat pas incidentit
Informacione të tjera të rëndësishme	*Mësimet e nxjerra*

Data	
Formulari depozitohet pranë autoritetit përgjegjës me: *E-mail (të skanuara) në adresën: incidente.raportimi@ere.gov.al*	

SHTOJCË NR. 3

Raportimi i vetëvlerësimit të operatorit mbi impaktin e incidentit të Sigurisë		
Kohëzgjatja e incidentit të sigurisë (ndërprerjes së shërbimit, interceptimit të komunikimeve, *software* të dëmshëm, modifikimi i të dhënave)	*Më tepër se 1 orë, por më pak se 2 orë*	*Më tepër se 2 orë*
Numri i përdoruesve të prekur nga incidenti ose % e tyre ndaj numrit total të përdoruesve		
→ 5%	*Mesatar*	*i lartë*
Në rast të një numri të panjohur të përdoruesve të prekur nga incidenti i sigurisë do të vlerësohet, zona gjeografike e shtrirjes së incidentit të sigurisë		
→ 20 km²		
Vlerësimi përfundimtar i impaktit:	**Mesatar**	**i lartë**