REPUBLIKA E SHQIPËRISË

ENTI RREGULLATOR I ENERGJISË

DRAFT-Strategjia për infrastrukturat kritike në sektorin e energjisë elektrike

Kjo strategji duhet të përdoret në përputhje me "Autoritetin Kombëtar për Çertifikimin Elektronik dhe Sigurinë Kibernetike"

Neni 1

Autoriteti

Enti Rregullator i Energjisë elektrike në bazë të nenit 18 të ligjit nr.43/2015 "Për sektorin e energjisë elektrike", ushtron funksionet rregullatore me qëllim promovimin 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. Bazuar në sa më sipër ERE konsideron sigurinë në hapësirën kibernetike si përgjegjësi e përbashkët me të licensuarit që operojnë në sektorin e energjisë elektrike për qëllime të furnizimit pandërpreje.

Neni 2

Qëllimi

Qëllimi i këtij dokumenti është të përcaktojë rregullat dhe masat që duhet të ndërmerren nga operatorët e infrastrukturave kritike në sektorin e energjisë elektrike për rreziqet e shkeljes apo dëmtimit të këtyre infrastrukturave në kuadër të operimit përmes platformave të ndryshme dixhitale.

Neni 3

Objekti

Kjo rregullore përcakton detyrimin e operatorëve që operojnë infrastrukturat kritike në sektorin e energjisë elektrike që të marrin masat e duhura gjatë projektimit, instalimit dhe funksionimit të rrjetit ose pajisjeve të përdorura prej tyre, në mënyrë që të garantojnë sigurinë, integritetin dhe funksionimin e qëndrueshëm të sistemit elektroenergjitik, si dhe të paraqesin pranë ERE, sipas

Aneks nr.2 dhe Aneks nr.3, çdo ndërhyrje, cënim ose incident në sigurinë dhe integritetin e rrjeteve të tyre të komunikimit elektronik apo çdo ndërhyrje , dëmtim që ka një impakt të konsiderueshëm në funksionimin e rrjeteve dhe/ose të shërbimeve të tyre për zbatimin e masave të sigurisë kibernetike për të mbrojtur infrastrukturën kritike dhe të rëndësishëm për të gjithë të licencuarit në aktivitetin e prodhimit transmetimit, shpërndarjes, të energjisë elektrike.

Neni 4

Termat e përdorur në Rregullore

Termat e përdorur në këtë dokument do të kenë kuptimin e përcaktuar në ligjin nr. 43/2015 "Për Sektorin e Energjisë Elektrike" dhe në ligjin nr. 2 /2017 "Për Sigurinë Kibernetike".

Neni 5

Rregulla të përgjithshme dhe parime bazë

1.Strategjia për infrastrukturat kritike në sektorin e energjisë elektrike është konceptuar në formën e një udhëzimi konform nenit 18 të Ligjit Nr. 43/2015 "Për Sektorin e Energjisë Elektrike" , Ligjit nr.2/2017 "Për Sigurinë Kibernetike" dhe VKM Nr.222, datë 26.04.2018, "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 për sektorin e energjisë elektrike është që përmes kuadrit tekniko ligjor të sigurohet furnizim i qëndrueshëm me energji elektrike dhe në përputhje me zhvillimet teknologjike, ligji nr.2/2017 "Për Sigurinë Kibernetike" ka për qëllim arritjen e një niveli të lartë 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 energjitik, përmes të cilave sigurohen shërbimet e licensuara.

b) Operatori i infrastrukturave kritike në sektorin e energjisë elektrike duhet të ndërmarrë masa të duhura dhe proporcionale, teknike dhe organizative ndaj sigurimit në internet për të menaxhuar rreziqet që paraqiten për sigurinë e rrjetit dhe informacionit në të cilat shërbimi i tyre thelbësor mbështetet, dhe për të parandaluar dhe minimizuar ndikimin e incidente në shërbimin thelbësor përmes partneritetit dhe bashkëpunimit midis Operatorëve dhe ERE.

2. Ky dokument mbështet 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 dhe vendos procese për të ndihmuar OEIK të demonstrojnë se ata po menaxhojnë rreziqet e sigurisë kibernetike në lidhje me shërbimet e ofruara. Këto procese përfshijnë kryesisht:

a. • Vetëvlerësimi nga OEIK,
b. • Identifikimi dhe hartimi i planit të masave
c. • Identifikimi dhe rishikimi i planeve të investimeve

2.a OEIK do të paraqesë vetëvlerësimin e tij në ERE dhe ky vetëvlerësim do të përmbajë një informacioni të detajuar të vetëvlerësimit të plotë të çdo rreziku domethënës të identifikuara dhe çdo propozim fillestar për trajtimin e rrezikut përfshirë deklarim për rezultatin e arritur duke identifikuar atë si 'Jo E arritur "ose" Pjesërisht e arritur " dhe "e Arritur" Operatorit nuk i kërkohet të paraqes asnjë provë mbështetëse ku rezultatet janë emërtuar "Arritur".

Ky informacion duhet të dorëzohet duke përdorur modelin e raportimit të vetëvlerësimit i cili gjendet në Aneksin. Nr.1.
Pasi të paraqitet informacioni ERE kur është e përshtatshme, mund të hyjë në diskutim me OEIK dhe të kërkoj informacione të mëtejshme për çështjet e raportuar për të mbështetur vlerësimet e tij. 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 lidhet është i paqartë ERE mund të kërkojë sqarime nga OEIK.

OEIK 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 OEIK të ketë përfunduar vetëvlerësimin e tyre, OEIK duhet të marrin në konsideratë fushat për përmirësim.

Në vetëvlerësimin fillestar, qëllimi kryesor është që OEIK të ndërmarrë një vetëvlerësim të saktë dhe të zhvillojë një plan përmirësimi, ku kërkohen përmirësime. Çdo vlerësim sipas statusit respektiv i arritur ose jo do të shoqërohet me shpjegimet përkatëse për çdo konkluzion. Këto raportime mund të jenë pjesë e auditimeve dhe inspektimeve të OEIK.

2.b Pas procesit për paraqitjen e Vetëvlerësimit të përcaktuara më lart, OEIK do zhvillojnë planet e tyre të masave. OEIK mund të kërkojë bashkëpunim me ERE siç përcaktohet më lart.

Planet e masave duhet të bazohen në vetëvlerësimet e OEIK duke identifikuar rreziqet në përputhje me menaxhimin e tyre të rrezikut dhe metodologjinë e riskut. Plani i përmirësimit duhet të përcaktojë kundërmasat e sigurisë kibernetike që OEIK 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 përmes planifikimit të biznesit. ERE, rast pas rasti, mund të kërkojë rishikimin e planit të masave nga OEIK në mënyrë që t'i ndihmojë ata në prioritarizimin dhe planifikimin e mbrojtjes nga rreziku kibernetik.

2.c OEIK duhet të zhvillojë një Sistem të Menaxhimit të Sigurisë kibernetike, për të menaxhuar rreziqet në mënyrën e duhur. Ky sistem do të sigurohet brenda afatit të përckatuar nga ERE sipas analizës dhe propozimit të OEIK, dhe mund të përfshijë ndër të tjera rekrutimin e ekspertëve në fushën e teknologjisë informatike 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 në internet për rreziqet e larta duhet të bazohet në raportin e varësisë, kompleksitetit rast pas rasti. Kjo mund të përfshijë:

a) Rishikimi i detyrimeve kontraktuale për palët e treta,
b) Vendosja e praktikave për laptopët inxhinierikë,
c) Vendosja e praktikave për përdorimin e mediave të lëvizshme,
d) Menaxhimi i ndryshimit të llogarive të paracaktuara të përdoruesve dhe fjalëkalimeve etj.

3. Pas paraqitjes së planit të parë të vetëvlerësimit dhe përmirësimit, ERE do të kryejë auditime/monitorime në vend.

Neni 6

Detyrime të operatorëve të infrastrukturave kritike

1.Për qëllime të kësaj strategjie detyrat e operatorëve të infrastrukturave kritike në sektorin energjitik përfshijnë :

a. Një OEIK duhet të marrë masat teknike dhe organizative për të menaxhuar rreziqet që mund ti shfaqen e që lidhen me sigurinë e rrjetit dhe të sistemeve të informacionit në të cilat mbështetet shërbimi i licensuar nga ERE, me qëllim sigurimin e vazhdimësisë së atyre shërbimeve.
b. Një OEIK 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 licensuar nga ERE, me qëllim të sigurimit të vazhdimësisë së këtyre shërbimeve.
c. Një OEIK ka për detyrë për të njoftuar incidentet pranë ERE 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, veprimarisë së licensuar.

2. Në përputhje me përcaktimet e pikës 1 të këtij neni, OEIK, do të raportojë periodikisht një herë në gjashtë muaj, brenda muajit Janar dhe Korrik për 6-mujorin paraardhës, sipas Aneksit 1 të kësaj rregulloreje për çështjet që lidhen me zbatimin e gërmes a, dhe b të pikës 1 të këtij neni dhe në çdo rast tjetër do të njoftojë sa më shpejt që të jetë e mundur dhe jo më vonë se 72 orë nga dita kur është marrë djeni nga OEIK për ndodhjen e incidentit të identifikuar sipas gërmës c të pikës 1 të këtij neni.

3. Faktorët kryesorë për vlerësimin e realizimit nga Operatori të detyrave sipas kësaj strategjie, do të përfshijnë një vlerësim nga ERE:
- nëse janë zbatuar apo jo masa të përshtatshme dhe propocionale të sigurisë për detyrat e sigurisë së OEIK.
- nëse incidentet i janë njoftuar ERE
Frekuenca e ndodhjes së një incidenti sipas gërmës c, pika 1, të nenit 6 në vetvete nuk do të thotë se ka pasur një dështim nga një operator për të përmbushur detyrat e tij të sigurisë ose detyrat e njoftimit.

4. Brenda 30 ditëve nga një incident i infrastrukturave kritike, OEIK duhet të paraqesë një raport të përgjithshëm për ERE. Brenda 60 ditëve nga një incident i infrastrukturave që po raportohet nga një OEIK, kjo e fundit pritet të paraqesë një raport të hetimit pas incidenteve. Në çdo rast OEIK mund të kërkojë rishikimin e datave sipas kësaj pike.

Neni 7

Raportimi

Infrastrukurat kritike do të raportojnë jo më vonë se 3 ditë pune nga momenti i zbulimit të incidentit të sigurisë për çdo rast që përbën një shkelje/ndërhyrje që ka cënuar sigurinë kibernetike të infrastrukturave kritike që i licensuari operon.
Grupi i punës i ngritur nga ERE përbërë nga përfaqësues të drejtorive teknike, me paraqitjen e informacioneve nga të licensuarit në rast të incidenteve të raportuara, do të diskutoj rastin e raportuar me të licensuarin 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 ligjzbatuese për veprimet e propozuara me qëllim shmangien apo uljen e numrit të incidenteve.

Në përputhje me informacionin e përgatitur nga grupi i punës, dhe analizës së tij Bordi i ERE mund të kërkoj auditime të mëtejshme dhe / ose inspektime për t'u siguruar se këto veprimet janë adresuar në mënyrë të duhur.
ERE mund të kërkojë informacion të detajuar për të mbështetur çdo vlerësim mbi pajtueshmërinë e veprimeve të të licensuarit me rregullat që lidhen me sigurinë e infrastrukturave kritike.

Nëse ERE konkludon se bashkëpunimi me OEIK nuk ka funksionuar ose është e qartë se nuk janë marrë masat e duhura për shmangien e incidenteve në infrastrukturat kritike, ERE do të njoftoj operatorin sipas një njoftimi që përmban:

- Dështimet e identifikuara,

- Hapat që duhen ndërmarrë për të korrigjuar dështimet, dhe periudhën kohore në të cilën ato duhet të realizohen.

Neni 8

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 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.

Neni 9

Dispozita përfundimtare

u miratua nga Bordi i Entit Rregullator të Energjisë me Vendimin nr… , datë. __/__/

ANEKSI 1

Raporti i vetëvlerësimit mbi mbrojtjen e infrastrukturave kritike dhe Menaxhimi i Riskut

Operatori do të raportojë mbi:
Politikat e Sigurisë së Informacionit të infrastruktave kritike që ai operon,
Menaxhimi i Riskut,
Rolet e sigurisë dhe përgjegjësitë e cila përfshin aftësinë e Zbulimit të Incidenteve dhe Aftësia e Rregullimit të Pasojave,
Siguria e aseteve të palëve të tjera të kontraktuara nga i licensuari,
Kualifikimet e personelit për identifikimin dhe reagimin ndaj sulmeve kibernetike.

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.

ANEKSI 2

Formulari për raportimin e një incidenti të sigurisë dhe/ose cënimit të integritetit	
Informacion Kontakti	*Emri i Sipermarresit:*
	Emri dhe Mbiemri i personit te ngarkuar me eleminimin e incidenteve te sigurise dhe/ose cenimit te integritetit:
	Pozicioni i Punes:
	Adresa:
	Telefon, e-mail:
Pershkrimi i Incidentit te Sigurise dhe/ose Cenimit te Integritetit	*Lloji:*
	Percaktimi se cila rrjete, sisteme ose sherbime preken na incidenti i sigurise:
	Koha e ndodhjes dhe kohezgjatja:
	Informacion rreth shkakut fillestar ose shkaqeve:
	Pershkrimin e incidentit (percaktoni te dhenat ne menyre sa me te detajuar):
	Numri i perafert i perdoruesve te prekur nga incidenti i sigurise ose cenimi i integritetit ose perqindja e tyre(%) nga perdoruesve total te rrjetit dhe/ose sherbimit:
	Zona Gjeografike e prekur nga incidenti i sigurise dhe/ose cenimi i integritetit (km²):
	Burimet e prekura
	Pasojat :

Menaxhimi i incidentit te sigurise dhe/ose cenimit te integritetit	*Veprimet e ndermarra(te planifikuara per tu ndermarre) per te eleminuar incidentin e sigurise dhe per te reduktuar pasojat e tij:*
	Masat pas incidentit
Informacione te Tjera te Rendesishme	*Mesimet e nxjerra*
Data	
Formulari depozitohet pranë Autoritetit Përgjegjës me: *E-mail (te skanuara) ne adresen: incidente.raportimi@ere.gov.al*	

ANEKSI 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**