Politika për Mbrojtjen e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit

Përmbajtja

1. Hyrje

Politika për Mbrojtjen e Infrastrukturës Kritike bazohet në legjislacionin në fuqi për sigurinë kibernetike, si dhe në objektivat dhe prioritetet e Strategjisë Kombëtare për Sigurinë Kibernetike dhe synon të garantojë mbrojtjen, qëndrueshmërinë dhe funksionimin e pandërprerë të sistemeve dhe aseteve që janë thelbësore për sigurinë kombëtare, rendin publik dhe stabilitetin ekonomik të vendit. Kjo politikë përbën një komponent të rëndësishëm të kuadrit kombëtar të sigurisë kibernetike, duke adresuar rreziqet dhe kërcënimet që cenojnë infrastrukturat kritike dhe të rëndësishme të informacionit.

Përmes nxitjes së bashkëpunimit ndërmjet sektorit publik dhe privat, politika synon të mbështesë zhvillimin dhe zbatimin e teknologjive, mekanizmave dhe praktikave më të mira në fushën e sigurisë kibernetike, me qëllim forcimin e mbrojtjes dhe rritjen e reziliencës së infrastrukturës kritike.

2. Qëllimi

Politika ka për qëllim:

- Të sigurojë mbrojtjen efektive të sektorëve të infrastrukturës kritike, përmes identifikimit, vlerësimit dhe menaxhimit të rreziqeve dhe kërcënimeve që mund të ndikojnë funksionimin e tyre;
- të zhvillojë dhe zbatojë strategji për parandalimin, zbulimin dhe reagimin ndaj sulmeve dhe incidenteve kibernetike që kërcënojnë integritetin, disponueshmërinë dhe konfidencialitetin e infrastrukturave kritike;
- Të krijojë një mbrojtjeje të fortë dhe të qëndrueshme për këto sisteme duke siguruar që ato të jenë të përgatitura për të përballuar dhe rikuperuar nga çdo kërcënim potencial.

3. Fusha e Zbatimit

Kjo politikë zbatohet për të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit, ku përfshihen sektorët e energjisë, transportit, shëndetësisë, administrata publike, bankar/financiar, infrastruktura digjitale, furnizimit me ujë, hapësinor, arsimor dhe çdo sektor tjetër që, në rast ndërprerjeje ose cenimi, do të shkaktonte pasoja të rënda në nivel kombëtar.

4. Parimet Themelore

- Zbatimi i kësaj politike mbështetet në disa parime bazë ne përputhje edhe me objektivat e përcaktuara në Strategjinë Kombëtare për Sigurinë Kibernetike. Mbrojtja e infrastrukturave kritike dhe të rëndësishme bazohet në një qasje proaktive, ku masat e sigurisë përcaktohen në përputhje me nivelin e kërcënimit dhe ndikimit potencial. Po ashtu, theksohet parimi i reziliencës, sipas të cilit infrastruktura duhet jo vetëm të mbrohet, por edhe të jetë e aftë të funksionojë dhe të rikuperohet pas incidenteve.
- Një tjetër parim thelbësor është bashkëpunimi ndërinstitucional publik privat, pasi pjesë e listës së infrastrukturave kritike dhe të rëndësishme operohen edhe nga subjekte private.

5. Elementët kryesore të Politikës

i. Identifikimi i Infrastrukturës Kritike: Përcaktimi i qartë i infrastrukturave që konsiderohen kritike, duke përfshirë, por pa u kufizuar në, sektorët e energjisë, transportit, shëndetësisë, telekomunikacionit, financave, furnizimit me ujë dhe shërbimeve qeveritare.

ii. Vlerësimi dhe Menaxhimi i Rrezikut: Kryerja e vlerësimeve periodike të rrezikut për të identifikuar kërcënimet dhe cenueshmëritë kibernetike që prekin infrastrukturën kritike, si dhe zhvillimi i masave për menaxhimin, trajtimin dhe zbutjen e tyre.

iii. Standardet e Sigurisë Kibernetike: Zbatimi i standardeve dhe kërkesave rregullatore të sigurisë kibernetike për sektorët e infrastrukturave kritike, përfshirë kërkesat për sistemet e informacionit, raportimin e incidenteve dhe kontrollin e përputhshmërisë.

iv. Partneriteti Publik-Privat: Nxitja e bashkëpunimit ndërmjet institucioneve publike dhe subjekteve private që zotërojnë ose operojnë infrastrukturë kritike, përmes ndarjes së informacionit, zhvillimit të ushtrimeve të përbashkëta dhe planifikimit të koordinuar të përgjigjes ndaj incidenteve kibernetike.Planet e Përgjigjes ndaj Incidenteve dhe Rikuperimit: Hartimi, zbatimi dhe përditësimi i planeve gjithëpërfshirëse për reagimin dhe rikuperimin nga incidentet kibernetike, duke përcaktuar qartë rolet, përgjegjësitë dhe protokollet e komunikimit gjatë situatave emergjente.

v. Investimi në Teknologjitë e Sigurisë Kibernetike: Implementimi i teknologjive të avancuara të sigurisë kibernetike për mbrojtjen e infrastrukturave kritike dhe rritjen e aftësive për zbulimin dhe parandalimin e sulmeve.

vi. Zhvillimi i kapaciteteve njerëzore: Fokusimi në trajnim dhe zhvillimin e kapaciteteve njerëzore në sigurinë kibernetike me qëllim rritjen e aftësive për menaxhimin dhe mbrojtjen e infrastrukturave kritike.

vii. Mekanizma të ndarjes së Informacionit: Krijimi i platformave dhe protokolleve për ndarjen e informacionit rreth kërcënimeve kibernetike, cënueshmëritë dhe incidenteve midis palëve të interesit të infrastrukturës kritike.

viii. Bashkëpunimi Ndërkombëtar: Angazhimi në bashkëpunime ndërkombëtare për të ndarë praktikat më të mira, informacionet e inteligjencës dhe strategjitë për mbrojtjen e infrastrukturës kritike globale.

ix. Kontrolle periodike të përputhshmërisë: Zbatimi i kontrolleve dhe vlerësimeve të rregullta për të garantuar përputhshmërinë e subjekteve të infrastrukturës kritike me politikat, standardet dhe kërkesat e sigurisë kibernetike.

x. Programe të Ndërgjegjësimit dhe Trajnimit: Zhvillimi i trajnimeve të rregullta të ndërgjegjësimit dhe ushtrimeve trajnuese për palët e interesit në sektorët e infrastrukturës kritike për kërcënimet kibernetike.

xi. Mbështetje në kërkim dhe zhvillim: Inkurajimi dhe mbështetja ne kërkim dhe zhvillim për teknologjitë e reja të sigurisë kibernetike dhe praktikat më të mira, të fokusuara veçanërisht për mbrojtjen e infrastrukturës kritike.

6. Referencat

Kjo politikë mbështetet në legjislacionin kombëtar për sigurinë kibernetike, Strategjinë Kombëtare për Sigurinë Kibernetike, si dhe në praktikat dhe standardet ndërkombëtare të njohura në fushën e mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit.

7. Frekuenca e Rishikimit

Ky dokument duhet të rishikohet të paktën një herë në vit ose kur ka ndryshime të rëndësishme në sistemin e menaxhimit të sigurisë së informacionit në institucion.