Politikat e Vlerësimit të Rrezikut Kibernetik

Përmbajtja

1. Hyrje

Politika e Vlerësimit të Rrezikut Kibernetik është thelbësore për garantimin e sigurisë në një mjedis kibernetik gjithnjë e më kompleks dhe të ekspozuar ndaj rreziqeve. Vlerësimi i rrezikut të sigurisë kibernetike, i realizuar nga strukturat përgjegjëse, përbën një proces kyç për identifikimin, analizimin dhe vlerësimin e kërcënimeve dhe cenueshmërive që prekin infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe interesat kombëtare.

Ky proces krijon bazën për hartimin dhe zbatimin e politikave dhe masave të sigurisë kibernetike, duke mbështetur zhvillimin e strategjive për menaxhimin dhe zbutjen e rreziqeve, si dhe duke kontribuar në forcimin e qëndrueshmërisë dhe mbrojtjen efektive të interesave kombëtare.

2. Qëllimi

Qëllimi i politikes Vlerësimit të Rrezikut të Sigurisë Kibernetike është identifikimi, analizimi, vlerësimi dhe prioritizimi i kërcënimeve dhe cenueshmërive që mund të ndikojnë në infrastrukturën kritike, shërbimet thelbësore dhe interesat kombëtare. Ky proces synon të mbështesë vendimmarrjen strategjike për menaxhimin dhe zbutjen e rreziqeve kibernetike, përmirësimin e masave ekzistuese të sigurisë, alokimin efikas të burimeve dhe forcimin e mbrojtjes së përbashkët të sigurisë kombëtare.

3. Fusha e zbatimit

Kjo politikë zbatohet nga Autoriteti Kombëtar për Sigurinë Kibernetike dhe është e detyrueshme për zbatim nga operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit sipas përcaktimeve ligjore në fuqi

4. Parimet e vlerësimit të rrezikut kibernetik

Vlerësimi i rrezikut kibernetik bazohet në parime themelore si një proces i strukturuar, sistematik dhe i vazhdueshëm, duke marrë në konsideratë probabilitetin e ndodhjes dhe ndikimin e mundshëm të kërcënimeve mbi asetet, shërbimet kritike dhe interesat kombëtare.

Vlerësimi kryhet në mënyrë proporcionale dhe të përshtatshme me kontekstin, rëndësinë e infrastrukturës, ndjeshmërinë e informacionit dhe nivelin e ekspozimit ndaj kërcënimeve, duke integruar aspekte teknike, organizative dhe njerëzore, duke siguruar një pamje gjithëpërfshirëse të rrezikut.

Procesi është transparent dhe i dokumentuar, duke garantuar gjurmueshmëri të analizës, vendimmarrjes dhe rezultateve, si dhe mundëson rishikim dhe auditim të mëvonshëm. Vlerësimi i rrezikut konsiderohet një proces dinamik, i cili rishikohet dhe përditësohet periodikisht për të reflektuar ndryshimet në mjedisin e kërcënimeve, teknologji dhe kapacitete.

5. Elementët e vlerësimit përfshijnë

i. Identifikimi i Kërcënimeve

Identifikimi i kërcënimeve kibernetike që prekin hapësirën kombëtare, përfshirë, por pa u kufizuar në, programet keqdashëse, sulmet ransomware, phishing, aktivitete kibernetike të sponsorizuara nga shtete dhe kërcënime të brendshme.

ii. Vlerësimi i Cenueshmërisë

Analizimi i cenueshmërive në rrjetet dhe sistemet qeveritare, sektorët e infrastrukturës kritike dhe ndërmarrjet private, me qëllim vlerësimin e nivelit të rrezikut dhe ekspozimit ndaj kërcënimeve të identifikuara

iii. Analiza e Rrezikut

Vlerësimi i mundësisë së ndodhjes dhe ashpërsisë së ndikimit të kërcënimeve që mund të shfrytëzojnë cenueshmëritë e identifikuara, duke duke vlerësuar ndikimin potencial te tyre ne sigurinë kombëtare në sigurinë kombëtare, ekonominë dhe sigurinë publike.

iv. Rishikimi i Qëndrimit Aktual të Sigurisë

Vlerësimi i masave ekzistuese të sigurisë kibernetike dhe efektivitetit të tyre, përfshin politikat, procedurat dhe kontrollet teknike, në adresimin dhe trajtimin e rreziqeve të identifikuara.

v. Rishikimi i Historisë së Incidenteve

Rishikimi dhe analizimi i incidenteve kibernetike të mëparshme, me qëllim identifikimin e dobësive sistemike dhe vlerësimin e kapaciteteve ekzistuese të reagimit.

vi. Konsultimi me Palët e Interesit

Angazhimi i institucioneve publike, subjekteve private dhe partnerëve ndërkombëtarë për mbledhjen e informacionit, inteligjencës dhe praktikave më të mira në fushën e sigurisë kibernetike.

vii. Rekomandimet për Zbutjen e Rrezikut

Hartimi i rekomandimeve për adresimin e rreziqeve të identifikuara, duke përfshirë masat teknike dhe organizative të bazuara në politikat dhe kërkesat rregullatore si dhe ngritjen e kapaciteteve dhe iniciativave ndërgjegjësuese.

viii. Alokimi i Burimeve

Mbështetja e procesit të alokimit të burimeve financiare, teknologjike dhe njerëzore të nevojshme në shërbim të menaxhimit dhe reduktimit të rreziqeve kibernetike në nivel kombëtar.

ix. Përditësimet e Rregullta dhe Monitorimi i Vazhdueshëm

Sigurimi i përditësimeve të rregullta për të reflektuar ndryshimet në peizazhin e kërcënimeve kibernetike dhe garantimi i mbikëqyrjes së vazhdueshme.

x. Raportimi dhe Komunikimi

Raportimi i gjetjeve, analizave dhe rekomandimeve te autoritetet përkatëse dhe palët e interesit, si dhe komunikimi i qartë dhe efektiv i rreziqeve dhe veprimeve të nevojshme për adresimin e tyre.

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 për vlerësimin dhe analizimin e rrezikut të sigurisë kibernetike.

7. Frekuenca e Rishikimit

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