Akademija kibernetičke sigurnosti HGK
Radionice za kategorizirane subjekte prema Zakonu o kibernetičkoj sigurnosti
24.3.2026., Split

PROGRAM

08:45 – 09:00 – Registracija i okupljanje

09:00 – 09:10 – Uvodni pozdrav

09:10 – 11:00 – Procjena rizika i upravljanje rizicima

11:00 – 11:20 – Pauza za kavu

11:20 – 13:15 – Procjena rizika dobavljača (Supply chain risk management)

13:15 – 13:45 – Pauza uz zakusku

13:45 – 15:00 – Provedba samoprocjene prema Zakonu o kibernetičkoj sigurnosti

15:00 – 15:30 – Uspostava sustava kontinuiteta poslovanja

Predavač; Marko Gulan, savjetnik za kibernetičku sigurnost

Radionica obuhvaća četiri tematske cjeline:

Procjena rizika i upravljanje kibernetičkim rizicima
Prvi dio radionice usmjeren je na uspostavu strukture upravljanja rizicima koja je usklađena s nacionalnim zakonskim zahtjevima.
Sudionici će kroz praktične primjere naučiti:

- kako identificirati i kategorizirati imovinu,
- kako mapirati prijetnje, ranjivosti i scenarije rizika,
- kako procijeniti vjerojatnost i posljedice,
- kako koristiti risk matrix modele koji zadovoljavaju regulatorne revizije,
- kako definirati kontrole, mjere i akcijske planove,
- kako voditi i održavati službeni registar rizika.

Poseban naglasak stavlja se na proporcionalnost, kako uspostaviti sustav koji je dovoljno robustan da zadovolji nadzor, ali i dovoljno jednostavan da bude održiv u manjim organizacijama.

Procjena rizika dobavljača (Supply Chain Risk Management)
Drugi dio radionice bavi se razvojem sustava za upravljanje rizicima trećih strana, što je jedan od najkritičnijih elemenata u kategoriziranim subjektima te jedna od najčešćih slabosti u nadzoru.
Sudionici će naučiti:

- kako strukturirati upitnik za dobavljače ovisno o vrsti usluge (IT, cloud, outsourcing, fizička sigurnost, konzultanti...),
- koje obvezne elemente mora sadržavati upitnik prema Zakonu o kibernetičkoj sigurnosti
- kako procijeniti odgovore i odrediti razinu rizika dobavljača,
- kako voditi evidenciju dobavljača i periodičkih provjera,
- kako integrirati rezultate procjene u vlastiti sustav upravljanja rizicima.

Poseban naglasak daje se na praktične primjere već korištenih i regulatorno prihvaćenih upitnika, kao i na metodologiju procjene kritičnih dobavljača.

Provedba samoprocjene prema Zakonu o kibernetičkoj sigurnosti
Treća komponenta radionice fokusira se na provedbu formalne **samoprocjene sukladnosti**, koja je jedna od temeljnih obveza kategoriziranih subjekata.
Sudionici će kroz ovaj modul:

- razumjeti cjelokupnu strukturu samoprocjene i obvezna područja koja obuhvaća,
- naučiti kako dokumentirati postojeće stanje, razinu implementacije kontrola i identificirane nedostatke,
- vidjeti koje dokaze je regulatorno prihvatljivo priložiti,
- naučiti kako izraditi akcijski plan i matricu zrelosti,

Ovaj dio radionice posebno je vrijedan jer organizacijama pomaže da realno procijene vlastitu razinu otpornosti, identificiraju rizike i nedostatke, a sve u obliku koji je potpuno kompatibilan s očekivanjima nadzora.

Format i rezultati radionice
Po završetku radionice polaznici dobivaju:

- predloške (risk register, upitnik za dobavljače, BIA obrazac, self-assessment strukturu),
- jasne smjernice za interne politike i procedure,
- pregled regulatornih očekivanja i konkretnih dokaza koje je potrebno imati,
- metodologiju koja je održiva, mjerljiva i jednostavno primjenjiva.

Uspostava sustava kontinuiteta poslovanja i Business Impact Analysis (BIA)
Četvrti dio radionice usmjeren je na planiranje kontinuiteta poslovanja, jedan od ključnih zahtjeva za sve kritične i važne subjekte. Radionica uključuje demonstraciju tipičnog BCP dokumenta, obrasce za BIA i prikaz najboljih praksi iz sektora kritične infrastrukture.

Ovaj program posebno je prilagođen organizacijama koje tek uspostavljaju sustav prema Zakonu o kibernetičkoj sigurnosti, ali i onima koje žele unaprijediti postojeću razinu sukladnosti i operativne otpornosti.

Radionica je idealna za organizacije koje grade sustav kibernetičke sigurnosti od temelja, ali i za one koje žele provjeriti ili unaprijediti postojeću razinu sukladnosti i pripremljenosti.