Institut za ekonomsku diplomatiju vas poziva na praktičnu radionicu

Izrada internih akata prema novom Zakonu o informacionoj bezbednosti

PRAKTIČNA IZRADA AKAKTA, PROCEDURE, EVIDENCIJE I 9 NOVIH MERA – IZRADA KOMPLETNE DOKUMENTACIJE PREMA NOVOM ZAKONU O IB

Dom kulture Studentski grad, Novi Beograd ili onlajn (ZOOM)
9. jul 2026. godine od 10h

Stupanjem na snagu novog Zakona o informacionoj bezbednosti („Sl. glasnik RS“, br. 91/25), značajno je proširen krug subjekata koji imaju obavezu primene naprednih mera zaštite, ali i nivo odgovornosti u njihovoj primeni. U praksi to znači da organizacije koje spadaju u kategoriju IKT sistema od posebnog i važnog značaja više ne mogu da se oslone na parcijalna ili formalna rešenja – već moraju imati **uređen, dokumentovan i funkcionalan sistem bezbednosti**, koji se može dokazati u svakom trenutku. Poseban izazov predstavlja činjenica da Zakon uvodi **9 NOVIH MERA**, ali i **dodatnu obavezu IZRADE VELIKOG BROJA DOKUMENATA, EVIDENCIJA I PROCEDURA,** koje postaju ključni dokaz usklađenosti u inspekcijskom nadzoru.

Kroz prizmu zakonskih novina, najvažnije teme koje ćemo obraditi su:

- Pregled **obaveza i postupanja** u skladu sa pozitivnim zakonodavstvom RS
- **Detaljna analiza** svih zakonskih obaveza koje operatori moraju ispuniti
- Implementacija **9 novih mera bezbednosti**
- **Kontinuirani nadzor**: obaveze, rokovi i konkretno postupanje radi stalne zaštite IKT sistema
- **Izrada operativne dokumentacije**: metodologija kreiranja organizacionih i kadrovskih mera zaštite
- **Upravljanje incidentima**: obavezna evidencija i prikupljanje podataka o pretnjama po informacionu bezbednost
- Pravilnici i procedure: **Izrada pisanih protokola o radu, upravljanju rizicima i kontroli pristupa** (Akt o proceni rizika i Akt o bezbednosti IKT sistema)
- **Plan kontinuiteta poslovanja (BCP)**: Metodologija očuvanja kritičnih funkcija i operacija preduzeća u slučaju nepredviđenih okolnosti
- **Plan oporavka od IKT incidenta i katastrofa (DRP)**: Strategija tehničkog povratka sistema u radno stanje
- **Godišnji izveštaj o proveri mera**: Finalni dokument koji potvrđuje efikasnost sprovedenih mera bezbednosti.

Krunski ishod obuke – Po završetku obuke, polaznici će biti u stanju da:

- samostalno izrade kompletnu zakonski propisanu dokumentaciju

Informacije: 011/3077612, 3077613, 063/509972;
prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;
www.economicdiplomacy.co.rs

- sprovedu 9 novih mera zaštite
- uspostave funkcionalan sistem IKT bezbednosti
- izbegnu potrebu za angažovanjem eksternih konsultanata
- obezbede potpunu dokumentacionu spremnost za nadzor

Predavačice:

1) **Olga Zorić**, ekspertkinja za korporativnu i informacionu bezbednost, specijalista za projektovanje složenih sistema zaštite i strateško usklađivanje poslovanja sa pravnim i zakonskim okvirima. Poseduje višegodišnje iskustvo u implementaciji integrisanih strategija koje spajaju fizičku i digitalnu bezbednost u neraskidivu celinu, obezbeđujući potpunu zaštitu korporativnih resursa.
2) **Dragana Jakovljević**, Ekspertkinja za informacionu bezbednost i upravljanje rizicima, specijalistkinja za transformaciju kompleksnih teorijskih pravila u praktične operativne procedure sa dugogodišnjim iskustvom. Njena ekspertiza osigurava da bezbednost postane živ proces, a ne samo administrativna obaveza. Fokusirana na primenu mera koje garantuju kontinuitet poslovanja i potpunu dokumentacionu spremnost za inspekcijski nadzor.

NASTAVNI PROGRAM

1) VAŽEĆI PROPISI
Zakon o informacionoj bezbednosti – novine i ključne obaveze
- Novine u odnosu na prethodni zakon i razlozi povećanja obima zahteva
- Subjekti koji imaju obaveze
- Usklađenost sa NIS2 direktivom

Uloga i odgovornost menadžmenta organizacije
- Informaciona bezbednost kao deo korporativne kulture i strategije
- Obaveze odgovornog lica u skladu sa Zakonom i reagovanje na incidente
- Kreiranje politike bezbednosti i kontrola njene primene
- Primena domaćih i međunarodnih standarda – ključne procedure

2) EVOLUCIJA RANJIVOSTI – SISTEMATIZACIJA PRETNJI KROZ AUTOMATIZACIJU
Evolucija ranjivosti IKT sistema – sistematizacija pretnji kroz automatizaciju
- ISO standardi kao temelj novog Zakona
- Evolucija rizika – više niste meta samo vi
- Industrijalizacija napada (AI & RaaS)
- Ranjivost lanca snabdevanja – od koga sve zavisimo
- Promena filozofije odgovornosti IT – Bezbednost subjekta
- Uloga novih autoriteta – Kancelarija za informacionu bezbednost i CERT
- Inspekcijski nadzor i dokumentacija
- Krovni dokument novog Zakona: Akt o proceni rizika i Akt o informacionoj bezbednosti

3) STRATEGIJA MAPIRANJA RIZIKA I POSTAVLJANJE NEPROBOJNIH PRAVILA ODBRANE

Akt o proceni rizika – Mapiranje pretnji i dijagnostika ranjivosti sistema

- Procedura upravljanja rizikom – metodologija: kako merimo opasnost
- Katalog pretnji – Lista savremenih opasnosti (AI botovi, RaaS, socijalni inženjering)
- Lista mera sigurnosti – odabir "lekova" za prepoznate pretnje
- Evidencija informacionih dobara, opreme i delova opreme – popis svega što branimo
- Procedura klasifikacije informacione imovine – Kategorizacija (Kritično-1 do Nisko -4)
- Matrica klasifikacije i šema poverljivosti informacija – Ko sme da vidi koji podatak
- Registar rizika po sektorima – Specifične ranjivosti HR-a, prodaje i finansija
- Plan tretmana rizika po sektorima – prioriteti: šta popravljamo odmah

Akt o IKT bezbednosti – operativa – pravila igre i tehnički bedemi odbrane

- Operativne procedure informacione bezbednosti
- Politika za kontrolu pristupa informacijama – ko, gde i kako ulazi u sistem
- Procedura za upravljanje sigurnošću i kontrola pristupa mrežama – tehničke barijere
- Procedura kontrole pristupa aplikacijama – zaštita softverskog jezgra firme
- Zaštita protiv malicioznog i prenosivog softvera – odbrana od virusa i botova
- Uputstvo za izradu rezervnih kopija – tehnička strategija čuvanja podataka (Backup)
- Evidencija nosača podataka – upravljanje USB stikovima i eksternim diskovima
- Politika i pravilnik za prenos opreme, medija i informacija van prostorija preduzeća
- Uputstvo za zaposlene o korišćenju IKT – edukacija i odgovornost svakog radnika
- Procedura i uputstvo za održavanje sistema – kako krpimo "rupe" (Patch management)

Dokazivost

- Zapisnici o sprovedenim procedurama – merama (potvrde o dodeljenim pristupnim šiframa, reversi za zaduženje laptopova, izveštaji o obavljenim backup-ima, zapisnici sa obuka zaposlenih u phishing-u ili logovi o ulasku u serversku salu)
- Periodična revizija

4) MEHANIZMI OTPORNOSTI – OSIGURANJE PREŽIVLJAVANJA I BRZ POVRATAK U RAD

Plan kontinuiteta poslovanja – BCP (fokus na ljude i procese)

- Plan obezbeđenja kontinuiteta p oslovanja – glavni dokument (Krovna strategija)
- Registar rizika i Plan tretmana rizika po sektorima
- Procedura klasifikacije informacione imovine (Kategorije 1-4) – prioriteti za spasavanje
- Politika i pravilnik za prenos opreme i informacija van prostorija
- Uputstvo za zaposlene o korišćenju IKT u toku vanrednog stanja

Plan oporavka usled katastrofe (DRP)

- Plan oporavka usled katastrofe (DRP) – glavni tehnički dokument
- Pregled IKT opreme (sa RTO i RPO parametrima) – najvažnija tabela
- Plan postupanja u slučaju incidenta – operativni protokol, ko šta radi u prvih 60 minuta napada
- Uputstvo za izradu rezervnih kopija (Backup) – osnova za "restore"
- Evidencija nosača podataka – gde su fizički bekapi i eksterni diskovi koji nam trebaju za

oporavak
- Procedura i uputstvo za održavanje sistema – koraci za proveru sistema naon što ga "podignemo iz mrtvih"

Izveštaj o proveri mera bezbednosti IKT sistema – godišnji

- Izveštaj o sprovedenim radnjama provere
- Zaključak o usklađenosti
- Zaključak o primeni memra
- Ocena nivoa bezbednosti
- Predlog korektivnih mera

Obuka je namenjena:

- Direktorima, pravnicima, menadžerima informacione bezbednosti, stručnim IT licima
- CISO (Chief Information Security Officer)
- Licima za zaštitu podataka o ličnosti, internim revizorima informacione bezbednosti

---

Način realizacije, kotizacija i popusti:

Nastava se može, **po sopstvenom izboru**, pratiti u nastavnoj sali (u prijatnom ambijentu Doma kulture Studentski grad na Novom Beogradu) ili on-line putem ZOOM platforme. Obe grupe učesnika slušaju nastavu u isto vreme.

1. **Za prisustvo u nastavnoj sali**, kotizacija iznosi 23.500,00 (+PDV) i obuhvata nastavu, nastavni materijal, sertifikat, direktno interaktivno učešće u predavanju, posluženje u pauzama.
2. **Za učešće putem ZOOM platforme** kotizacija iznosi 21.500 (+PDV). Nastava se prati u realnom vremenu, zajedno sa učesnicima koji su fizički prisutni u sali. Pitanja se postavljaju putem chat-a, a predavači će na njih odgovoriti nakon pauze ili na kraju predavanja.

Popusti:

- Za sve prijave i avansne uplate odobrava se popust od 5%
- Za dva i više učesnika iz iste organizacije, odobrava se dodatnih 10% popusta
- Za učesnike naših ranijih seminara iz oblasti IKT bezbednosti, odobrava se dodatni popust od 5% (popust za lojalnost)

Informacije i prijavljivanje:

Prijavu možete izvršiti klikom na dugme "Prijavite se" gde možete popuniti elektronsku prijavu ili preuzeti obrazac u .doc formatu i poslati ga na bilo koju od naših e-mail adresa

Za dodatne informacije kontaktirajte nas na:

063/509972, 063/506097, 011/3077613
prijava@economicdiplomacy.co.rs; ied.bg@mts.rs