Upravljanje bezbjednosnim i informacionim rizicima

Opis kursa (Naučićete)

Kurs pruža osnovna i napredna znanja i veštine za upravljanje bezbjednosnim i informacionim rizicima koji su aktuelni i mogu se ispoljiti u gotovo svakoj kompaniji. Kurs omogućava polaznicima da se postepeno upoznaju sa vrstama IT rizika i njihovom pravilnom klasifikacijom, kao i prevencijom i zaštitom od rizika koji se mogu ispoljiti kako u okviru interno razvijenih i podržanih IT sistema tako i kod eksternalizovanih IT usluga.

Neka od pitanja na koja će vam kurs pružiti odgovore su kako adekvatno tretirati uočene informacione i bezbjednosne rizike, šta je potrebno propisati i ko je za to odgovoran, na šta treba obratiti pažnju prilikom eksternalizcije IT usluga i koje su to kritične stavke svakog ugovora, zatim kako bezbjedno upravljati internim razvojem i pravilno implementirati kripto algoritme i različite metode autentifikacije. Tokom kursa ćemo uraditi analizu pozitivnih, ali i negativnih iskustava velikih kompanija prilikom procjene IT rizika, angažovanja eksternih partnera i kreiranja ugovora.

Kome je kurs namijenjen

Kurs je namijenjen menadžmentu kompanije, rukovodiocima i zaposlenima u službi za upravljanje kontinuitetom poslovanja, IT službi i službi za bezbjednost informacionog sistema, odgovornim licima za zaštitu poslovnih informacija i upravljanje operativnim rizicima, internim i eksternim revizorima, osobama zaduženim za kreiranje i kontrolu IT ugovara i praćenje rizika nad eksternalizovanim IT procesima, zaposlenima koji rade na razvoju softvera, poslovnih i klijentskih aplikacija, zatim zaposlenima u poslovnim sektorima koji hoće da povećaju nivo kontrole nad svojim IT procesima ili se bave razvojem novih usluga kroz digitalizaciju poslovanja (digitalno poslovanje, mobilne usluge itd.), kao i svima koji imaju potrebu da zaštite i sačuvaju informacije o klijentima i poslovanju zbog visokog stepena odgovornosti, regulatornih zahtjeva i rizika u svakodnevnom poslovanju.

Cilj kursa

Cilj kursa je da steknete osnovno i napredno znanje u upravljanju bezbjednosnim i IT rizicima, kao i da bolje razumijete IT kontrole koje se primjenjuju za smanjivanje ili otklanjanje uočenih rizika.

Potrebno predznanje

Potrebno je osnovno razumijevanje IT sistema i poslovnih procesa.

Trajanje kursa

2 dana (12 h)

Sadržaj kursa

Upravljanje IT rizicima

- Metodologija procjene IT rizika
- Prijetnje i ranjivosti u IT sistemu
- Upravljanje bezbjednosnim i IT rizicima i GDPR
- Da li su IT rizici operativni rizici?
- Rizik od otkaza u IT sistemu – dostupnost servisa
- Klasifikacija IT rizika
- Uticaj IT rizika na poslovne procese i razvoj novih proizvoda
- Testiranje i produkcija

- IT standardi i preporuke
- Pravilno definisanje i adekvatna primjena internih IT propisa

Bezbjednosni rizici u informacionom sistemu

- Bezbjednosne prijetnje i ranjivosti
- Procjena verovatnoće i uticaja bezbjednosnih rizika
- Ljudski faktor i uticaj na procjenu rizika
- Klasifikacija i označavanje informacija
- Definisanje bezbjednosnih rizika tokom internog razvoja
- Zaštita informacija, kripto algoritama i napredne metode autentifikacije
- Bezbjednosne provjere prije puštanja softvera u realizaciju
- Najbolja svjetska praksa i bezbjednosni standardi

Eksternalizacija IT usluga

- Bezbjedno poslovanje kroz eksternalizaciju IT usluga
- Saradnja sa partnerima i analiza rješenja/ponuda
- Procjena budućeg partnera i uticaj eksternalizacije na kritične IT procese u kompaniji
- Obaveze eksternih partnera
- Kreiranje i odobravanje ugovora
- Kritične stavke ugovora i održavanje IT opreme
- Kontrola procesa kod eksternih partnera

Primjeri iz prakse

- Da li ste uradili klasifikaciju IT rizika?
- Da li ste u ugovoru za IT održavanje pokrili sve što Vam je važno?
- Analiza rizika – interni razvoj ili eksternalizacija
- Analiza primjera loše procjene rizika – ne sagledavanje cijele slike
- Analiza najčešćih IT rizika i rješenja za prevenciju – praktični primjeri