SPECIALIST ZA UPRAVLJANJE TVEGANJ INFORMACIJSKE VARNOSTI

OPIS

Vedno večje količine zaupnih informacij, ki jih kopičijo organizacije, se zbirajo, obdelujejo in shranjujejo v računalniških sistemih. Njihovo varovanje postaja vedno pomembnejša poslovna, kot tudi etična in pogosto pravna zahteva.

Področje informacijske varnosti se v zadnjih letih izjemno povečuje in razvija; kar je logična posledica vedno večjih tveganj, ki jih poslovanju predstavlja naraščajoč spletni kriminal. Skoraj ni velike organizacije, ki ne bi bila njegova žrtev.

Zato je nuja podjetij in organizacij, da aktivno in stalno skrbijo za ustrezno varovanje informacijskih sistemov.

Za vse, ki ste v podjetjih odgovorni za informacijsko varnost predstavljamo novo intenzivno praktično izobraževanje.

Komu je seminar namenjen?

Program je namenjen odgovornim za informacijsko varnost v podjetjih in ustanovah.

Izobraževanje je namenjeno vsem odgovornim za informacijsko varnost v podjetjih in ustanovah. Strokovnjaki iz prakse bodo podali praktične usmeritve glede:

- aktualnih varnostnih tveganj,
- planiranja ustreznih preventivnih varovalnih ukrepov,
- pravilnega ukrepanja v primeru incidentov,
- omejitev, ki jih nalaga zakonodaja na področju varstvo osebnih podatkov in novosti, ki jih glede tega lahko pričakujemo v naslednjem letu.

Vsebina

Celovit pristop k varovanju informacij

1. del: Informacijsko premoženje organizacije, ocena tveganj, zakonodaja

- Tipi informacij
- Opredelitev informacijskega premoženja
- Grožnje informacijski varnosti
- ZVOP-1, Uredba EU 2016/679, Direktiva EU 2016/680, Direktiva EU 2016/1148
- Metodologije ocene tveganj

- Ocena tveganj kot podpora odločanju

2. del: Ščitenje informacijskega premoženja, dobra praksa

- ISO/IEC 27001, ISO 22301
- Strategija kibernetske varnosti RS
- Priprava življenjskih varnostnih politik, PDCA krog
- Vpeljava varnostnih politik, različni pristopi
- Posodabljanje politik (prilagajanje spremembam)
- Redno ozaveščanje in izobraževanje zaposlenih

Gradivo prejmete na prvi delavnici.

- Slovenska zakonodaja, ki ureja osebnostne pravice delavcev in pooblastila delodajalcev
- Nekateri vidiki zakonske ureditve varstva osebnih podatkov
- Informacijski pooblaščenec in inšpekcijski nadzor
- Posebne zahteve zakona o varstvu osebnih podatkov
- Dopusten obseg nadzora zaposlenih s strani delodajalcev
- Problematika evidenc prisotnosti zaposlenih na delovnem mestu na podlagi prstnih odtisov
- Praksa Informacijskega pooblaščenca v zvezi z varovanjem zasebnosti in osebnih podatkov v delovnih razmerjih
- Diskriminacija in spolno nadlegovanje na delovnem mestu
- Posebnosti v javnem sektorju
- Praktični nasveti delodajalcem v primeru konfliktnih situacij
- Občutljivi osebni podatki v delovnopravnih razmerjih
- Zasebnost in obdelava osebnih podatkov z vidika informacijskih tehnologij
- Najpogostejša vprašanja v zvezi z varovanjem osebnih podatkov
- Praktični primeri, obrazci in drugi vzorci za takojšnjo uporabo na CD-ju

Upravljanje incidentov

1. del: Varstvo osebnih podatkov in poslovnih skrivnosti

- Osebni računalniki, delovno okolje
- Mobilne naprave
- Komunikacijska oprema
- Fizični mediji, papirna dokumentacija

2. del: Ukrepanje v primeru incidentov

- Preiskava incidenta (ugotavljanje trenutnega stanja in rekonstrukcija dogodkov)
- Zavarovanje dokazov
- Nadaljnji pravni ukrepi

Človeški dejavnik varovanja informacij

1. del: Najpogostejši incidenti in preventiva (s primeri iz slovenskega in tujega okolja)

- Splet – brskalniki, zlorabe storitev
- E-pošta – vsiljena pošta, priponke, učinkovita raba
- Kriptovirus – demonstracija v živo, prepoznavanje, ukrepanje
- Okuženi in odtujeni mediji – USB ključi

2. del: Odgovornost in komunikacija

- Preiskava incidenta (ugotavljanje trenutnega stanja in rekonstrukcija dogodkov)
- Zavarovanje dokazov
- Nadaljnji pravni ukrepi

AVTORJI

mag. Filip Božič

Mag. Filip Božič je certificiran etični heker in vodilni presojevalec za področje upravljanja varovanja informacij ter neprekinjenega poslovanja. Predava na usposabljanju za DPOje ter številnih konferencah in izobraževalnih programih. Široko tehnično znanje na področju informatike že dve desetletji nadgrajuje z organizacijskimi pristopi k ščitenju informacijskega premoženja v Sloveniji in širše.

Žiga Primc

Žiga Primc je certificirani etični heker (CEH), detektiv z licenco št. 162 in varnostni strokovnjak za varnost informacij v organizaciji, ki že vrsto let preiskuje in rešuje vdore v organizacije, kraje poslovnih skrivnosti, izsiljevanja organizacij in izobražuje zaposlene v organizacijah na področju varovanja informacij vseh oblik.

SPLOŠNI POGOJI

IZOBRAŽEVALNI PROGRAMI

Kotizacijo je po prejemu predračuna treba poravnati najmanj tri dni pred izvedbo programa. Za proračunske porabnike veljajo plačilni pogoji v skladu z zakonodajo o javnih plačilih. Pisna odpoved udeležbe je mogoča do deset delovnih dni pred izvedbo programa, pri čemer vam zaračunamo stroške administracije v višini 20 % kotizacije; v primeru kasnejše odjave vam kotizacijo zaračunamo v celoti. Lahko pa se programa udeleži drug udeleženec. Odpoved udeležbe zaradi bolezni je mogoča le s predloženim zdravniškim potrdilom. Pridržujemo si pravico do odpovedi – v tem primeru kotizacijo povrnemo v celoti. S pisno prijavo na izobraževanje sprejemate ta določila in splošne pogoje.