CYBER SECURITY – NOVE ZAKONODAJNE ZAHTEVE NA PODROČJU KIBERNETSKE VARNOSTI V PRAKSI

Strožja pravila kibernetske varnosti in širitev kroga zavezancev za njihovo upoštevanje!

Datum: 19.6.2024

OPIS

CYBER SECURITY – NOVE ZAKONODAJNE ZAHTEVE NA PODROČJU KIBERNETSKE VARNOSTI V PRAKSI

Ste vedeli, da bomo podjetja in organizacije podvrženi korenitim spremembam zaradi temeljnega amandmaja o kibernetski varnosti na nivoju EU? Prav tako se spreminja nacionalna zakonodaja.

Evropska direktiva NIS 2* je stopila v veljavo 16.1.2023 (v nacionalno zakonodajo mora biti prenešena čez 21 mesecev), priprava nanjo pa bo še bolj zahtevna kot na GDPR, zato je zelo smiselno **pravočasno pričeti z ustreznimi prilagoditvami**! NIS 2 zajema številne sektorje, ki NIS 1 niso bili podvrženi!

*Direktiva Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji

Kazni so astronomske – do 10 milijonov EUR oz. 2% letnega prometa (kar je višje), če hkrati kršite NIS 2 in GDPR, pa vas čaka **dvakratna kazen!** Za skladnost z novimi pravili ne bo več odgovoren samo IT, temveč **odgovarja neposredno vodstvo organizacije.**

18. 4. 2023 je bila sprejeta tudi novela Zakona o Informacijski varnosti (ZInfV), ki zaradi vedno večjih kibernetskih groženj povečuje zaščito centralnega informacijsko-komunikacijskega sistema državne uprave. **Zakon širi krog zavezancev in predpisuje nove zahteve in potrebne ukrepe!**

Zakaj se seminarja morate udeležiti?

- Seznanjeni boste s **temeljno spremembo na področju kibernetske varnosti,** ki prihaja v naša podjetja in organizacije iz EU
- Spoznali boste **stroga pravila** in vedeli, **kako se širi krog podjetij,** ki jih mora upoštevati
- Razumeli boste **celo vrsto korakov, ki jih boste morali izvesti** (analiza tveganja informacijskega sistema, določitev varnostne politike, krizno upravljanje prometa, revizija kibernetske varnosti, varnost komunikacije v sili…)
- Vedeli boste, kdo so »**povezani subjekti**« in kakšne **nove zahteve prinaša ZInfV** za vse, ki se **kakor koli povezujete s centralno-informacijskim sistemom** (kontaktna oseba, analiza obvladovanja tveganja, ocena sprejemljive ravni tveganja, navodila in postopki za obvladovanje incidentov, protokol obveščanj, izvajanje minimalnega obsega varnostnih ukrepov …)
- V praksi boste **obvladovali IT tveganja** oz. znali pravilno in učinkovito ravnati v primeru incidentov
- V svoji organizaciji boste **ustrezno varovali podatke** tako v digitalnem kot fizičnem okolju!

Komu je seminar namenjen?

Direktorjem oz. vodjem organizacij, informatikom, IT specialistom, skrbnikom sistemov, korporativnim pravnikom, vodjem ekip, tako iz zasebnega kot javnega sektorja.

Predavatelj:

dr. Miha Dvojmoč

Pooblaščenec za varstvo osebnih podatkov (DPO), pravni svetovalec podjetjem in direktorjem glede njihovih pravic, obveznosti in odgovornosti ter podpornih dejavnosti njihovem poslovanju, predsednik Društva za zasebno varstvo in državljansko samovarovanje, soustanovitelj Inštituta za organizacijsko vedenje in predsednik Detektivske zbornice Republike Slovenije.

Vsebina

- Direktiva NIS 2 o doseganju visoke ravni kibernetske varnosti – kdo, kaj, kako
- Roki, nova obvezna poročila o incidentih, kazni (kazni za NIS2 – GDPR)
- Kako korak za korakom implementirati smernice v vaši organizaciji
- Kako izvesti analizo tveganja informacijskega sistema (korak za korakom)
- Kako vzpostaviti varnostno politiko in implementacijo smernic po novih pravilih
- Šifriranje in varnost komunikacije (varnost glasovne in besedilne komunikacije, večstopenjska verifikacija…)
- Razširjene zahteve Zakona o informacijski varnosti (ZInfV) in implementacija v prakso
- Obvladovanje tveganj in incidentov – kako v praksi upravljati s tveganji, prepoznavati aktualne IT grožnje,
- Tehnologije za zaščito pred IT napadi in zagotavljanje stalnega nadzora nad tehnologijo
- Strateški pristopi zagotavljanja IT varnosti
- Kako ustrezno varovati podatke – tako v kibernetskem kot fizičnem okolju; kontrole za izboljšanje informacijske varnosti

Preverite še ostala izobraževanja iz - IT in varnost podatkov. Pomagali vam bodo razjasniti številne dileme iz prakse.

IN-HOUSE izobraževanje

Izobraževanje lahko izvedemo samo za vaše zaposlene na sedežu vašega podjetja.

>> Pošljite povpraševanje

AVTORJI

dr. Miha Dvojmoč

Pooblaščenec za varstvo osebnih podatkov (DPO), pravni svetovalec podjetjem in direktorjem glede njihovih pravic, obveznosti in odgovornosti ter podpornih dejavnosti njihovem poslovanju, predsednik Društva za zasebno varstvo in državljansko samovarovanje, soustanovitelj Inštituta za organizacijsko vedenje in predsednik Detektivske zbornice Republike Slovenije.

SPLOŠNI POGOJI

SEMINARJI

Kotizacijo je po prejemu predračuna treba poravnati najmanj tri dni pred izvedbo seminarja. Za proračunske porabnike veljajo plačilni pogoji v skladu z zakonodajo o javnih plačilih. Pisna odpoved udeležbe je mogoča najkasneje tri delovne dni

pred izvedbo seminarja. Udeleženci, ki po tem roku prekličejo udeležbo ali se seminarja ne udeležijo, niso upravičeni do povrnitve kotizacije oz. so dolžni poravnati celotno kotizacijo. Lahko pa na seminar pošljejo drugega udeleženca. Odpoved udeležbe zaradi bolezni je mogoča le s predloženim zdravniškim potrdilom. Pridržujemo si pravico do odpovedi seminarja – v tem primeru kotizacijo povrnemo v celoti. S pisno prijavo na izobraževanje sprejemate ta določila in splošne pogoje.

POSEBNE UGODNOSTI

Posebne ugodnosti

- drugi udeleženec **10 % popusta,**
- tretji in nadaljnji udeleženci **20 % popusta,**
- 10 % popusta na strokovne priročnike in izobraževalne portale.

NE SPREGLEJTE: 20 % popust za mikropodjetja, fizične osebe in društva! Uporabite Kodo za popust: MICRO20

Navedeni popust se ne sešteva z drugimi popusti, razen s popustom za več udeležencev izobraževanj. Kodo uporabite v košarici ali jo pripišite.